[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 7/58 (2006.01)

[12] 发明专利说明书

专利号 ZL 200480041636.5

[45] 授权公告日 2010 年 1 月 27 日

[11] 授权公告号 CN 100585552C

[22] 申请日 2004.2.12
[21] 申请号 200480041636.5
[86] 国际申请 PCT/JP2004/001486 2004.2.12
[87] 国际公布 WO2005/078573 日 2005.8.25
[85] 进入国家阶段日期 2006.8.14
[73] 专利权人 日立超大规模集成电路系统株式会社
地址 日本东京都
[72] 发明人 村中雅也
[56] 参考文献
CN1434375A 2003.8.6
JP2003 - 332452A 2003.11.21
WO02/45139A1 2002.6.6
US5963104A 1999.10.5
审查员 欧阳琦

[74] 专利代理机构 北京市金杜律师事务所
代理人 季向冈

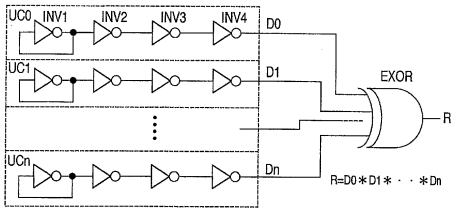
权利要求书 5 页 说明书 34 页 附图 22 页

[54] 发明名称

随机数发生方法和半导体集成电路器件

[57] 摘要

一种半导体集成电路器件，包括多个单位电路和信号变化检测电路，所述单位电路包括：以彼此相同的制造过程作为相同形态形成的第一和第二逻辑电路、将叠加在所述第一逻辑电路和第二逻辑电路的阈值电压的差电压上的噪声放大并形成 2 值信号的放大电路；所述信号变化检测电路，响应从所述多个单位电路输出的多个 2 值信号中的任意一个信号的变化，形成输出信号，该器件将多个从所述信号变化检测电路输出的 2 值信号进行组合发生随机数。



1. 一种随机数发生方法，其特征在于：

实现上述随机数发生方法的半导体芯片或半导体集成电路器件，包括在半导体基板上配置的多个单位电路和输入来自该多个单位电路的输出的信号变化检测电路，上述单位电路作为一组包含噪声检测对象电路、和输入该噪声检测对象电路的输出信号的放大电路，

各上述噪声检测对象电路包括以相同的制造过程形成为相同形态的第一翻转逻辑电路和第二翻转逻辑电路，

当上述多个单位电路和上述信号变化检测电路处于工作状态时，执行以下处理：

在各所述单位电路中，由上述放大电路将叠加在所述第一翻转逻辑电路和第二翻转逻辑电路的阈值电压的差电压上的噪声放大并形成2值信号，

所述信号变化检测电路，响应从所述多个单位电路的每一个输出的2值信号中的任意一个信号的变化，形成输出信号，

组合多个从所述信号变化检测电路输出的2值信号，生成随机数。

2. 根据权利要求1所述的随机数发生方法，其特征在于：

所述第一翻转逻辑电路、第二翻转逻辑电路，各自由具有第一和第二输入的逻辑门电路构成；

所述第一翻转逻辑电路所包含的逻辑门电路的输出与该逻辑门电路的第一输入连接；所述第二翻转逻辑电路所包含的逻辑门电路的第一输入与所述第一翻转逻辑电路所包含的逻辑门电路的输出连接；

所述放大电路由多个具有第一输入和第二输入的逻辑门电路构成，前一级逻辑门电路的输出与下一级逻辑门电路的第一输入连接，从而所述放大电路具有上述多个逻辑门电路串联连接的结构，

对构成所述第一翻转逻辑电路、第二翻转逻辑电路以及放大电路的逻辑门电路的第二输入分别提供动作控制信号时，使所述多个单位电路为工作状态。

3. 根据权利要求2所述的随机数发生方法，其特征在于：

上述半导体芯片或上述半导体集成电路器件还包括生成动作控制信号的顺序电路，

与上述动作控制信号对应地，依次使所述多个单位电路变为工作状态，串行输出全部单位电路的输出信号，由所述信号变化检测电路发生1位的随机数。

4. 根据权利要求3所述的随机数发生方法，其特征在于：

所述信号变化检测电路包括异或电路，接受从与上述动作控制信号对应地变为上述工作状态的单位电路依次顺序输出的输出信号形成所述随机数。

5. 根据权利要求3所述的随机数发生方法，其特征在于：

根据与所述1位随机数对应的全部单位电路的输出信号的组合，生成对上述半导体芯片或上述半导体集成电路器件的识别信号。

6. 根据权利要求1所述的随机数发生方法，其特征在于：

上述半导体芯片或半导体集成电路器件还包括算术方式的随机数发生电路，

将所述信号变化检测电路生成的随机数提供给上述算术方式的随机数发生电路；

从所述算术方式的随机数发生电路将来自所述信号变化检测电路的随机数作为初始值生成随机数。

7. 一种随机数发生方法，其特征在于：

实现上述随机数发生方法的半导体芯片或半导体集成电路器件中在半导体基板上配置有算术方式的随机数发生电路、多个单位电路、输入来自该多个单位电路的输出的信号变化检测电路，上述单位电路作为一组包含噪声检测对象电路、和输入该噪声检测对象电路的输出信号的放大电路，

各上述噪声检测对象电路包括以相同的制造过程形成为相同形态的第一翻转逻辑电路和第二翻转逻辑电路，

在工作状态下执行以下处理：

在各上述单位电路中，由上述放大电路将叠加在所述第一翻转逻辑电路和第二翻转逻辑电路的阈值电压的差电压上的噪声放大并生成2值信号；

将多个从多个上述单位电路的每一个输出的位所构成的信号提供给上述信号变化检测电路；

所述算术方式的随机数发生电路将从上述信号变化检测电路提供的多个位所构成的信号作为初始值生成随机数。

8. 一种半导体集成电路器件，其特征在于，包括：

多个单位电路，所述单位电路包括：以彼此相同的制造过程作为相同形态形成的第一和第二翻转逻辑电路、将叠加在所述第一翻转逻辑电路和第二翻转逻辑电路的阈值电压的差电压上的噪声放大并生成2值信号的放大电路；

信号变化检测电路，响应从所述多个单位电路的每一个输出的2值信号中的任意一个信号的变化，生成输出信号；

根据从所述信号变化检测电路输出的2值信号生成随机数。

9. 根据权利要求8所述的半导体集成电路器件，其特征在于：

所述第一、第二翻转逻辑电路和所述放大电路，各自由具有第一和第二输入的逻辑门电路构成；

所述第一翻转逻辑电路所包含的逻辑门电路的输出与该逻辑门电路的第一输入连接；

所述第二翻转逻辑电路所包含的逻辑门电路的第一输入与所述第一翻转逻辑电路所包含的逻辑门电路的输出连接；

对所述第一和第二翻转逻辑电路所对应的逻辑门电路的第二输入，提供动作控制信号；

所述放大电路中，多个逻辑门电路的第一输入和输出串联连接，对所述放大电路的逻辑门电路的第二输入提供所述动作控制信号。

10. 根据权利要求9所述的半导体集成电路器件，其特征在于：

还包括生成动作控制信号的顺序电路，

与所述动作控制信号对应地，依次使所述多个单位电路变为选择

状态；

在所述多个单位电路的输出部，设置所述信号变化检测电路。

11. 根据权利要求10所述的半导体集成电路器件，其特征在于：

所述信号变化检测电路包含异或电路，接受从与上述动作控制信号对应地变为上述选择状态的上述单位电路依次输出的输出信号生成所述随机数。

12. 根据权利要求11所述的半导体集成电路器件，其特征在于：

所述逻辑门电路是CMOS结构的逻辑门电路，通过所述动作控制信号使单位电路变为非工作状态时，使下一级的门电路的P沟道MOSFET为截止状态。

13. 根据权利要求11所述的半导体集成电路器件，其特征在于：

所述多个单位电路配置为矩阵；

在配置为矩阵的各单位电路的输入部，设置具有第一输入和第二输入的逻辑门电路，对第一输入和第二输入提供行和列选择信号，形成动作控制信号，通过输出该动作控制信号使构成所述第一翻转逻辑电路和第二翻转逻辑电路的逻辑门电路变为选择状态；

对构成所述各单位电路的放大电路的逻辑门电路的第二输入，传递来自配置在行方向的前级的单位电路的输出信号，所述放大电路在所述动作控制信号为非选择状态时，把来自前级的单位电路的输出信号放大并传递。

14. 根据权利要求13所述的半导体集成电路器件，其特征在于：

构成所述单位电路的MOSFET的栅极长度和栅极宽度，比构成包含所述信号变化检测电路或顺序电路的其他逻辑电路的MOSFET的栅极长度和栅极宽度大。

15. 根据权利要求11所述的半导体集成电路器件，其特征在于：

所述顺序电路包括连续多次选择相同的单位电路的测试模式；

在所述测试模式中，设置对从相同的单位电路多次输出的输出信号中形成不同的输出的单位电路的数量进行计数的电路；当所述形成不同的输出信号的单位电路的数量为大于等于1时，将半导体集成电

路器件判断为合格品。

16. 根据权利要求8所述的半导体集成电路器件，其特征在于：

还包括在半导体基板上配置的多个电路功能块，

多个上述单位电路和上述信号变化检测电路形成在上述半导体基板上，

上述所生成的随机数提供给上述电路功能块。

17. 一种利用随机数的设备，该设备包括个人电脑、移动电话、网络设备、无线通信设备、加密和复合器件、玩具或游戏机，其特征在于：

上述设备中安装的半导体芯片或半导体集成电路器件，包括在半导体基板上配置的多个单位电路和输入来自该多个单位电路的输出的信号变化检测电路，上述单位电路作为一组包含噪声检测对象电路、和输入该噪声检测对象电路的输出信号的放大电路，

各上述噪声检测对象电路包括以相同的制造过程形成为相同形态的第一翻转逻辑电路和第二翻转逻辑电路，

在工作状态下，利用执行以下工作而生成的随机数：

在各所述单位电路中，由上述放大电路将叠加在所述第一翻转逻辑电路和第二翻转逻辑电路的阈值电压的差电压上的噪声放大并形成2值信号，

所述信号变化检测电路，响应从所述多个单位电路的每一个输出的2值信号中的任意一个信号的变化，形成输出信号，

组合从上述信号变化检测电路输出的多个2值信号。

随机数发生方法和半导体集成电路器件

技术领域

本发明涉及随机数发生方法和半导体集成电路器件，尤其涉及适合于半导体制造技术的随机数发生方法及用于其半导体集成电路器件有效的技术。

背景技术

近年来，在网络化和IT化急速扩大的社会中，加密技术和认证技术等安全技术的重要性正在提高。作为这些技术的重要元素之一，随机数被经常使用。现在，基于若干种基本原理的随机数发生电路已被实用化。作为面向高度信息安全的超小型真随机数发生电路的例子，有“东芝检查”Vol.58·8（2003）（第一在先技术）。此外，在日本特开2003-173254号公报（第二在先技术）中记载有利用开关RS触发器的电源而取得的不确定输出的随机数发生电路。

发明内容

比较随机数发生电路的性能的要素，有随机数的质量（不规则性）、电路面积、功耗及响应时间（发生新的随机数所需要的时间）等，但是现有的随机数发生电路都有优点和缺点。随机数有2种，即用计算机的算法等发生随机数的伪随机数、使用自然界的物理现象发生随机数的真随机数。一般，后者的质量高。真随机数具有偶然性、非再现性、不可预测性等特长，但是需要复杂的电路和元件，不适合应用在简单的器件中。例如，在上述的第一在先技术中提出的技术是真随机数发生电路，但是需要工艺（蚀刻工序）的变更及控制。此外，由于上述第二在先技术利用了电源接通时的过渡状况下的现象，所以使随机数的不规则性下降的原因在设计阶段是不可预测的，难以保证

随机数的质量。

因此，本发明的一个目的在于，提供不进行制造工艺的变更，就能以小面积发生质量高的随机数的随机数发生方法以及具有随机数发生电路的半导体集成电路器件。本发明的另一个目的在于，提供实现低功耗的随机数发生方法和具有该随机数发生电路的半导体集成电路器件。本发明的上述以及其他目的和新特征，将通过本说明书的描述和附图得到明确。

对本申请中公开的发明中代表性的概要进行简单说明，则如下所述。即一种随机数发生方法，其特征在于：实现上述随机数发生方法的半导体芯片或半导体集成电路器件，包括在半导体基板上配置的多个单位电路和输入来自该多个单位电路的输出的信号变化检测电路，上述单位电路作为一组包含噪声检测对象电路、和输入该噪声检测对象电路的输出信号的放大电路，各上述噪声检测对象电路包括以相同的制造过程形成为相同形态的第一翻转逻辑电路和第二翻转逻辑电路，当上述多个单位电路和上述信号变化检测电路处于工作状态时，执行以下处理：在各所述单位电路中，由上述放大电路将叠加在所述第一翻转逻辑电路和第二翻转逻辑电路的阈值电压的差电压上的噪声放大并形成2值信号，所述信号变化检测电路，响应从所述多个单位电路的每一个输出的2值信号中的任意一个信号的变化，形成输出信号，组合多个从所述信号变化检测电路输出的2值信号，生成随机数。

附图说明

图1是表示本发明的装在半导体集成电路器件中的真随机数发生电路的基本概念的电路图。

图2是说明图1的真随机数发生电路的动作原理图。

图3是表示本发明的真随机数发生电路的一个实施例的基本电路图。

图4是表示图3的真随机数发生电路的一个实施例的具体电路图。

图5是用于说明图3的真随机数发生电路的动作的一个例子的波形图。

图6是表示图4的真随机数发生电路的信号变化检测电路的一个实施例的具体电路图。

图7是表示本发明的真随机数发生电路的另一个实施例的电路图。

图8是用于说明图7的真随机数发生电路的动作的一个例子的概念波形图。

图9是表示本发明的真随机数发生电路及其元素电路的一个实施例的电路图。

图10是表示本发明的真随机数发生电路及其元素电路的另一个实施例的电路图。

图11是用于说明图9的真随机数发生电路的动作的一个例子的概略波形图。

图12是表示本发明的真随机数发生电路的另一个实施例的概念图。

图13是表示图12的初始值发生电路的一个实施例的电路图。

图14是表示图12的初始值发生电路的另一个实施例的电路图。

图15是用于说明图13和图14的初始值发生电路的动作的波形图。

图16是表示本发明的真随机数发生电路的另一个实施例的电路图。

图17是表示本发明的真随机数发生电路的一个实施例的电路图。

图18是用于说明图17的真随机数发生电路中设置的测试电路动作的一个例子的时序图。

图19是表示本发明的真随机数发生电路的一个实施例的电路图。

图20是图19的真随机数发生电路的动作波形图。

图21是表示本发明的真随机数发生电路的一个实施例的电路图。

图22是表示本发明的真随机数发生电路的输出部的另一个实施例的电路图。

图23是图21所示的真随机数发生电路的动作波形图。

图24是表示本发明的真随机数发生电路的一个实施例的芯片结构图。

图25是表示本发明的半导体集成电路器件的一个实施例的框图。

图26是表示本发明的半导体集成电路器件的另一个实施例的框图。

图27是表示本发明的真随机数发生电路的另一个实施例的结构图。

图28是表示图27所示的真随机数发生电路的动作的一个例子的时序图。

图29是表示应用本发明的IC卡的一个实施例的外观图。

图30是表示本发明的装在IC卡上的IC卡用芯片的一个实施例的概略框图。

图31是表示应用本发明的非接触型IC卡的一个实施例的框图。

图32是由本发明的真随机数发生电路发生真随机数的二维分布图。

图33是表示图4的真随机数发生电路的变形例的具体电路图。

图34是表示图1所示的真随机数发生电路的基本概念的变形例的电路图。

图35是表示图1所示的真随机数发生电路的基本概念的其他变形例的电路图。

具体实施方式

为了进一步详细说明本发明，参照附图进行说明。

图1表示本发明的装在半导体集成电路器件中的真随机数发生电路的基本概念的电路图。图1所示的CMOS反相电路INV1~INV4在半导体集成电路器件的设计和制造上，在现实可控制的范围内，具有彼此相同的特性。关于使多个反相器具有彼此相同的特性的技术，以下进行简要说明。

在CMOS反相电路中，可理解为其特性概略地由构成它的P沟道型MOSFET和N沟道型MOSFET的相对电导决定。按照此观点，由沟道宽度W和沟道长度L的比W/L相同但尺寸不同的MOSFET，也能构成相同特性的CMOS反相器。但是，由半导体集成电路器件的制造离差引起的对电特性的影响，对于不同尺寸的元件不同。

在本实施例中，这样的多个CMOS反相电路INV1~INV4中的每一

个，最好使构成其的元件彼此即P沟道类型MOSFET彼此和N沟道类型MOSFET彼此具有相同的构造、相同的尺寸。当然这些元件按照相同元件在相同工艺下统一制造的半导体集成电路器件的特征来制造。据此，多个CMOS反相电路INV1~INV4均等地受到由半导体集成电路器件的制造上的加工尺寸的离差、各种层的厚度离差、杂质浓度离差等制造离差带来的影响。

如图1所示，使输入输出短路的CMOS反相电路INV1的输出电压达到逻辑阈值电压。如果全部CMOS反相电路具有完全相同的电特性，则4个反相电路INV1~INV4的逻辑阈值电压相等。但是，这只是理想的状态，在实际的半导体元件中，由于存在稍微的特性差异，所以各反相电路INV1~INV4的逻辑阈值电压发生差异。

可以认为，作为CMOS反相电路的阈值的离差的原因，MOS晶体管特性的离差是支配性的。而且，作为MOS晶体管特性的离差的原因，可列举出MOS晶体管栅极宽度、栅极绝缘膜厚度、决定导电的杂质浓度及其分布等。这些离差可分为宏观部分和微观部分。作为宏观部分，有相同批内的多个晶圆间的栅极宽度离差等。

在本发明中，主要考虑微观部分的离差，研究配置在比较接近的位置上的元件之间的离差。这样的微观的离差，可以作为比较接近的元件间随机发生的离差而观测到。

即：认为图1的反相电路INV1、INV2的逻辑阈值的离差也是随机的。该逻辑阈值的离差如后所述，在发生真随机数方面是不希望的，与之相对应，按照其他观点，半导体元件具有的特征的特性离差能作为固有的识别信息而利用。即、当使用CMOS反相电路时，逻辑阈值中发生的离差能够视为在N沟道类型MOSFET具有的离差中加上了P沟道类型MOSFET具有的离差所得的，离差范围扩大，能够有效地进行识别编号和识别信息的发生。但是，该事实在发生响应半导体元件的各节点上发生的噪声的真随机数方面是不希望的。

在图1所示的概念图中，将4个反相电路INV1~INV4作为基本电路（或单位电路）UC0，将CMOS反相电路INV1的输入和输出短路，形

成CMOS反相电路INV1的逻辑阈值电压VLT1。该逻辑阈值电压VLT1提供给反相电路INV2的输入。在反相电路INV2中，将其逻辑阈值电压VLT2作为参考电压，进行与上述逻辑阈值电压VLT1的电压比较和放大动作。然后，反相电路INV2的输出信号由串联的反相电路INV3和INV4构成的放大电路进一步放大，并变换为2值信号。

在理想的条件下，使得基本电路的第一反相电路INV1被短路的输入输出节点的电压（逻辑阈值电压VLT1）和第二反相电路INV2的逻辑阈值电压VLT2相等地进行设计、制造，但是实际上由于存在上述的工艺离差，所以不一定一致。

当电子在半导体内移动时，由于不规则的运动，所以发生电信号噪声，虽然其很小。该现象在第一反相电路INV1、第二反相电路INV2中都会发生，但是如上所述，在VLT1=VLT2那样的理想条件下，第一反相电路INV1的电信号噪声由第二反相电路INV2放大，第二反相电路的输出信号的振幅反映电信号噪声。由于电信号噪声进行完全无序的运动，所以从第二反相电路INV2取得的输出信号可以说是真随机数。

即：如图2（a）所示，当单位电路UC0的第一反相电路INV1和第二反相电路INV2的逻辑阈值电压VLT1、VLT2一致时，能够将电信号噪声Vnz翻转放大，并作为输出信号Vout取出。须指出的是，在该图中，省略第二反相电路INV2的电信号噪声，并包含在第一反相电路INV1的电信号噪声Vnz中。因此，第一反相电路INV1的电信号噪声Vnz由第二反相电路INV2翻转放大。而第二反相电路INV2的输出信号Vout再由第三和第四反相电路INV3、INV4放大，在第四反相电路INV4的输出中，最终取出电源电压电平的振幅的逻辑电平的信息。

但是，电信号噪声Vnz极小，实际上构成各反相电路INV1、INV2的MOS晶体管的特性由于上述的原因而存在离差，所以不能说基本电路UC0的第一和第二反相电路INV1、INV2的逻辑阈值电压VLT1、VLT2一定相等。

即，如图2（b）所示，单位电路UC0的第一反相电路INV1和第二

反相电路INV2的逻辑阈值电压VLT1、VLT2之间存在ΔV那样的基于工艺离差的差电压ΔV，当上述第二反相电路INV2的逻辑阈值电压VLT2总比上述电信号噪声Vnz的振幅大时，上述第二反相电路INV2的输出信号Vout总为高电平。因此，单独观察上述单位电路UC0时，并不保证第二反相电路INV2的输出信号Vout总反映上述的电信号噪声Vnz。

因此，一般考虑添加用于修正上述2个逻辑阈值电压VLT1、VLT2的上述工艺离差的微调或补偿电路，但是存在电路变得复杂，或消耗电流增大的问题。

本发明人着眼于晶体管特性的离差是随机正态分布的，如图1所示，发现如果观察多个基本电路，则第一反相电路INV1和第二反相电路INV2的特性极其相等的组合以一定概率存在，这样的基本电路如图2（a）所示，成为敏感地对电信号噪声Vnz作出反应的电路。

即、如图2(c)的阈值电压分布图所示，已知反相电路INV1、INV2的逻辑阈值电压VLT1、VLT2成为正态分布。如果组合2个反相电路INV1和INV2，则二者的差VLT1-VLT2成为原来的逻辑阈值电压VLT1、VLT2的方差的2倍的正态分布。第一反相电路和第二反相电路的逻辑阈值电压的差VLT1-VLT2比电信号噪声Vnz的振幅小的基本电路存在的概率由反相电路逻辑阈值电压VLT的方差、电信号噪声电压的振幅Vnz决定。基本电路群中所包含的噪声、即反映电信号噪声的基本电路的平均数是构成基本电路群的基本电路的数量乘以上述概率而取得的数。

在图1中，如果把UC0~UCn等多个基本电路的输出D0~Dn输入到以异或电路为代表的信号变化检测电路EXOR中，则其输出R对所连接的基本电路UC0~UCn的输出信号D0~Dn中的任意一个的变化都作出反应而翻转。

在上述多个基本电路UC0~UCn中至少存在一个第一反相电路和第二反相电路的特性极其相等的基本电路，将由第一反相电路和第二反相电路的特性极其相等的基本电路组成的多个基本电路群的各输出，输入到信号变化检测电路EXOR中。如果基本电路UC0~UCn的输

出D0~Dn中的任意一个变化，异或电路那样的信号变化检测电路EXOR的输出R就翻转。即，当信号变化检测电路EXOR的输入为基本电路的输出时，输出成为反映该基本电路的电噪声的真随机数。在基本电路群中即使存在多个第一反相电路和第二反相电路的特性极其相等的组合的基本电路，由于各基本电路的电信号噪声不相关连，所以信号变化检测电路EXOR的输出R同样是随机数，能取得更高质量的真随机数。在图1所示的逻辑表达式R=D0*D1*…*Dn中，*的记号表示异或记号。

图3表示本发明的随机数发生电路的一个实施例的基本电路图。在本实施例中，上述图1的反相电路INV1~INV4替换为2输入的“与非”（NAND）门电路。将上述门电路G1的一个输入与输出结合。将门电路G1的公共连接的输入输出与门电路G2的一个输入连接。门电路G2的输出与门电路G3的一个输入连接。门电路G3的输出与门电路G4的一个输入连接。而且，对门电路G1~G4的另一个输入公共地提供动作控制信号ACT。

图1的反相电路INV1~INV4能视为上述“与非”门电路G1~G4的逻辑门电路的一种。这是因为是进行把输入信号翻转的逻辑动作。如图1所示，使用反相电路INV1~INV4时，反相电路INV1和INV2，在第一级侧，在逻辑阈值电压VLT附近工作，在电源电压VDD和电路的接地电位之间，流过直流电流。在本发明中，如上所述，由于利用元件的工艺离差引起的逻辑阈值电压的正态分布，因此，有必要使较多的单位电路工作，所以在实现低功耗上，不能忽略上述反相电路INV1和INV2中的直流电流。

而如本实施例那样使用门电路G1~G4时，各门电路G1~G4在使动作控制信号ACT为低电平（逻辑0）那样的非激活电平时，与不同于上述动作控制信号ACT的另一个输入信号无关，使输出信号为高电平（逻辑1），在各门电路G1、G2中不发生直流电流。即，在实施例的电路中，在需要随机数的时刻，使上述动作控制信号ACT成为高电平（逻辑1）那样的激活电平。据此，各门电路G1~G4，进行响应不同

于上述动作控制信号ACT的另一个输入信号形成翻转信号的反相电路的动作。据此，通过使上述动作控制信号ACT为高电平，进行与图1的基本电路图同样的动作。

图4表示图3的真随机数发生电路的一个实施例的具体电路图。门电路G1由输出节点N1和电路的接地电位之间串联的N沟道MOSFETQ1和Q3、上述输出节点N1和电源电压VDD之间并联的P沟道MOSFETQ2和Q4构成。上述MOSFETQ1和Q3的栅极公共连接，作为第一输入。上述MOSFETQ2和Q4的栅极公共连接，作为第二输入。其他门电路G2~G4也由与上述相同的电路构成。

上述门电路G1~G4在半导体集成电路器件的设计和制造上，在现实可控制的范围内，具有彼此相同的特性。以下简要说明使多个门电路具有彼此相同的特性的技术。在门电路G1~G4中，作为其特性的逻辑阈值由构成它的P沟道MOSFET和N沟道MOSFET决定。在该观点中，能由沟道宽度W和沟道长度L的比W/L相同，但尺寸不同的MOSFET构成相同特性的CMOS门电路。但是，由于半导体集成电路器件的制造离差所引起的对电特性的影响，对于不同尺寸的元件不同。

在本实施例中，多个门电路G1~G4中，构成它的元件彼此，即P沟道类型MOSFET彼此和N沟道类型MOSFET彼此具有相同的构造、相同的尺寸。当然这些元件按照相同的元件在相同的工艺下统一制造的半导体集成电路器件的特征制造。据此，多个门电路G1~G4均等承受半导体集成电路器件的制造上的加工尺寸的离差、各种层的厚度离差、杂质浓度离差等制造离差引起的影响，并且逻辑阈值电压也具有正态分布。

在图3所示的实施例中，从门电路G2输出2个门电路G1和G2的逻辑阈值的大小的判断输出。通过在这样的信号传递和放大路线中叠加上述电信号噪声，取得反映为这样的电信号噪声的输出信号。即、门电路G2被短路的输入输出节点的电压（相当于逻辑阈值电压）作为门电路G2的输入偏压而提供，把反映为上述电信号噪声的输出信号由后

级的门电路G3、G4放大，取得CMOS电平的2值信号。因此，因为门电路G3、G4只进行放大动作，所以没必要像门电路G1、G2那样，P沟道类型MOSFET彼此和N沟道类型MOSFET彼此具有相同的构造、相同的尺寸，但是在本实施例中，主要从电路设计的观点出发，由相同的构造、相同的尺寸构成。

图5表示用于说明图3的真随机数发生电路的动作的一个例子的波形图。在图5中，省略信号传递路线中的电信号噪声。动作控制信号ACT如果从低电平变为高电平，上述门电路G1~G4实质上变为工作状态，门电路G1的输出节点N1变为与逻辑阈值对应的电压。须指出的是，将为此所需要的时间称作收敛时间。门电路G2根据逻辑阈值判断节点N1的电压，决定输出节点N2的电位。在例子中，门电路G1的逻辑阈值比门电路G2的逻辑阈值稍大一些，所以通过门电路G2的放大动作，节点N2的电压变为比上述节点N1小的电压。该节点N2的电压由门电路G3放大，如节点N3那样，变为高电平。然后，由门电路G4进一步放大，如节点N4那样，到达电路的接地电位VSS。

上述节点N1和N2的电位差很小，如果那里发生的电信号噪声变为节点N2的电位以下，输出信号就翻转。即、与上述图2（a）相同，发生使节点N1和N2的电位差翻转的电信号噪声时，反过来说，在具有只有由于电信号噪声使节点N1和N2的电位差关系颠倒这样的微小电压差的门电路G1和G2组合的基本电路中，输出能发生反映这样的基本电路的电噪声的真随机数。当然，能发生上述真随机数是经过收敛时间之后。如果是收敛时间内，受到各与非门的节点的过渡状态的影响，难以取得反映本来微小的电噪声的真随机数。

在本实施例中，在电路为停止状态即动作控制信号ACT为低电平时，图3的N沟道MOSFETQ3、Q7、Q11、Q15变为截止状态，能抑制使用上述CMOS反相电路时的穿透电流。此外，使用与非（NAND）电路作为门电路的优点是因为是CMOS逻辑LSI的标准元件，所以不限定应用的产品。即完全由逻辑记述型电路构成，所以电路设计变得容易。

在图4的实施例中，动作控制信号ACT与串联的N沟道MOSFETQ3、Q7、Q11、Q15的栅极连接，但是也可以与N沟道MOSFETQ1、Q5、Q9、Q13连接，节点N1、N2、N3与N沟道MOSFETQ3、Q7、Q11、Q15的栅极连接。

在晶体管电平电路记述中重要的是各NAND元件中的MOSFET的信号连接位置。在上述停止状态下，各门电路G1~G4的输出即节点N1、N2、N3的电位自动变为电源电压，所以具有能防止这些信号的连接目标的P沟道MOSFET的NBTI的特性变动的效果。

MOS晶体管有时由于阈值电压依存于如电场强度和温度那样的电场应力，而发生不希望地变动。特别是称作NBTI（Negative Bias Temperature Instability负偏置温度不稳定性）的现象是在P沟道MOSFET中显著表现的现象。作为防御对策，经常使用在目标之外的时间中使PMOS的栅极上外加的电压为高电压的方法。在本实施例中，根据上述动作控制信号ACT的高电平，进行逻辑阈值判断动作，在该逻辑阈值判断动作以外时，使动作控制信号ACT为低电平，使栅电压为固定电压，从而为P沟道MOSFET的栅极提供电源电压。据此，P沟道MOSFET中，栅极、漏极、源极和衬底（沟道）全部变为与电源电压相等的相同电位，能极力抑制上述MOSFET的时间经过变化引起的逻辑阈值的变动。这在通过组合各电位电路的输出信号，取得识别信息方面特别有效。

而在随机数发生电路中，具有以下特征：基本不受上述元件特性的变动或电源电压的变动影响。在本实施例的随机数发生电路中，如上所述，比较多的单位电路中至少存在一个门电路G1和G2的逻辑阈值电压从上述电信号噪声来看是相等的。上述元件特性的变动或电源电压的变动在由多个构成的单位电路群的全部中发生，即使在某单位电路中，门电路G1和G2的逻辑阈值电压从上述电信号噪声来看不是相等的，相反的，在其他单位电路中，，门电路G1和G2的逻辑阈值电压从上述电信号噪声来看是相等的。

图33表示图4的真随机数发生电路的变形例。为了抑制图33（a）

的与非门电路G1和G2（相当于上述图1的反相电路INV1和INV2）的电特性离差，构成NAND的晶体管的沟道长度L和沟道W都比标准尺寸（通常工艺的最小尺寸）大。通过使有关的晶体管的L以及W增大，能抑制晶体管的栅极的加工误差引起的特性离差。此外，能抑制MOS晶体管的栅极正下方的杂质浓度引起的统计性变动（把它称作“涨落现象”）。在近年的尖端工艺中，相同芯片上的MOS晶体管的电特性离差中，来自加工误差的涨落现象的影响是支配性的。

构成与非门电路G1和G2的各晶体管尺寸不需要是公共的，但是对与电路动作时的状态有关的，换言之，把对上述有效状态下的逻辑阈值的决定带来影响的P沟道MOSFETQ2（Q6）和N沟道MOSFETQ1、Q3（Q5、Q7）优先增大。各与非门电路G1和G2的对应的MOSFET需要是相同的形状。

此外，作为放大电路工作的门电路G3和G4不需要如上述那样设定，但是在电路设计或元件布局上使用与电路G1和G2相同的元件可使电路简单，在后面描述的隐藏随机数发生电路的存在方面是有利的。

图33（b）表示能取得与图33（a）同样的效果的其他实现方法的电路。使用3输入与非门，对激活状态下的逻辑阈值的决定带来影响的P沟道MOSFET和N沟道MOSFET各为2个，抑制上述涨落现象的影响。其优点是：不用特别设计特殊尺寸的MOS晶体管，用标准尺寸的门构件就能实现。

须指出的是，上述图3、图4和图33都是用与非（NAND）门构成基本电路，代替与非门，也可以是或非（NOR）门。但是，此时的相关基本电路在动作控制信号ACT为低电平（逻辑0）时变为有效。如上所述，引起被称作NBTI的电场应力的恶化现象在P沟道MOSFET中显著。可是，在其他元件例如多晶硅FET或有机晶体管中，有关的恶化现象不是P沟道型晶体管中，而是在N沟道型晶体管中显著时，优选的使用或非（NOR）门。

须指出的是，在图3所示的实施例中，将各单位电路UC0~UCn内

的与非门G2、G3、G4分别连接的公用动作控制信号ACT与电源VDD连接，总为高电平（逻辑1），据此，本实施例具有的基本功能不变。

图6表示图3的真随机数发生电路的信号变化检测电路EXOR的一个实施例的具体电路图。在本实施例中，异或电路EX0~Exn纵列连接，构成上述信号变化检测电路EXOR。对接受单位电路UC0的输出信号D0的异或电路EX0的另一个输入，虽然未特别限制，但是提供低电平（逻辑0）那样的固定值。对接受下一段单位电路UC1的输出信号D1的异或电路EX1的另一个输入，提供上述异或电路EX0的输出信号。以下，对接受第n+1个单位电路UCn的输出信号Dn的异或电路EXn的另一个输入，提供上述异或电路EXn-1的输出信号。

据此，上述n+1个单位电路UC0~UCn的输出信号D0~Dn中的任意一个变化，就与它对应，与它对应的异或电路EX的输出信号变化，通过上述串联的异或电路，异或电路EXn的输出信号R变化。即上述输出信号R成为反映单位电路（基本电路）的电噪声的真随机数。

作为上述信号变化检测电路EXOR，当用逻辑门电路构成时，虽然使用上述多个异或电路也很方便，但是并不局限于此，只要能检测输出信号D0~Dn的逻辑电平的变化，就可以是任意的。例如能采用通过输出信号D0~Dn、延迟信号，形成1脉冲的各种实施方式。

图7表示本发明的真随机数发生电路的另一个实施例的电路图。在本实施例中，单位电路UC0~UCn使用解码器DEC在时间上分散工作。而且，使用一个异或电路EX、一个触发器FF，把多个单位电路UC0~UCn的输出的异或逻辑累加，从而取得真随机数RR。须指出的是，通过把异或变更为复杂的逻辑，能取得发生模式更难以解读的真随机数。

上述解码器DEC虽未特别限制，但是由计数器和解码器构成。即用计数器对时钟CLK计数，把计数输出进行解码，发生使单位电路UC0~UCn依次变为工作状态的动作控制信号DEC0~DECn。或者，使用移位寄存器，根据时钟CLK依次把与选择信号相对应的初始值移位，形成使单位电路UC0~UCn依次变为工作状态的动作控制信号

DEC0~DECn。

为了使单位电路UC0~UCn依次变为工作状态，如果以单位电路UC0为例进行说明，则对门电路G1和G2提供作为动作控制信号的解码输出DEC0。作为放大电路的门电路G3和G4在上述门电路G1和G2通过动作控制信号DEC0变为工作状态时，对与之相对应的输出信号进行放大动作，当上述对门电路G1和G2通过动作控制信号DEC0变为非工作状态时，进行对前级的单位单元的输出信号的通过且传输动作。

与它对应的门电路G2的输出信号传递到门电路G3的一个输入，前级的单位电路的输出信号传递到另一个输入。门电路G4的一个输入是与它对应的门电路G3的输出信号，另一个输入是与电源电压对应的高电平。据此，门电路G4实质上作为反相电路而工作。第一段的单位电路UC0的门电路G3的另一个输入固定为与电源电压对应的高电平。

图8表示用于说明图7的真随机数发生电路的动作的一个例子的概念波形图。通过解码器DEC，与初级的单位电路UC0对应的动作控制信号DEC0变为高电平的选择电平，形成由门电路G1和G2形成并由门电路G3和G4放大的输出信号D0。在单位电路UC1~UCn中，由于上述动作控制信号DEC1~DECn是低电平的非选择电平，所以相当于门电路G2的门电路的输出信号全部为高电平。因此，相当于门电路G3的门电路进行作为反相电路的动作，只把来自前级电路的输出信号进行放大。结果，上述初级的单位电路UC0的输出信号D0通过上述单位电路UC1~UCn，传递给异或电路EX。即使D1～Dn的电平依从于D0的电平。

通过解码器DEC，如果与第二个单位电路UC1对应的动作控制信号DEC1变为高电平的选择电平，则与上述相同，形成基于与门电路G1和G2对应的2个门电路的输出信号并由门电路G3和G4放大的输出信号D1。即在上述第一段的单位电路中，由于选择信号DEC0的低电平，门电路G2的输出信号变为高电平，把输出信号D0固定在高电平。因此，在上述的单位电路UC1中，由门电路G3、G4进行放大动作。以下，输出信号D1与上述相同，通过后级一侧的单位电路中作为放大电

路的门电路，传递给异或电路EX。即、使D2～Dn的电平依从于D1的电平。第三个以后的单位电路UC2~UCn的选择动作也与上述相同。

图7的实施例电路的实际波形与图8不同。即在单位电路UC0为非选择状态时，输出信号D0为高电平。在上述DEC1变为非选择电平的同时，输出信号D0形成与非选择状态对应的高电平的输出信号。在单位电路UC1~UCn变为非选择电平时，各输出信号D1~Dn也一起变为高电平。因为难以理解如果与非选择状态对应，忠实地表现输出信号D0~Dn的电平，上述单位电路UC0~UCn就按顺序工作，输出依次（串行）输出，所以忽略单位电路UC0~UCn的非选择状态下的输出电平的变化，如图8所示那样。

在图7的实施例电路中，表示包含（n+1）个单位电路（基本电路）的单位电路群，在（n+1）个基本电路中，至少存在大于等于一个第一门电路G1（第一反相电路INV1）和第二门电路G2（第二反相电路INV2）的特性极其相等的组合的单位电路。如上所述，单位电路群中包含的第一门电路G1和第二门电路G2的特性极其相等的组合的单位电路数量越多，取得的随机数的质量越高。为了使单位电路群中包含的第一门电路G1和第二门电路G2的特性极其相等的组合的单位电路数量为足够的数量，需要提高第一门电路G1和第二门电路G2的特性极其相等的组合的单位电路存在的概率，使单位电路群中包含的单位电路的数量成为与有关的概率平衡的适当的数。第一门电路G1和第二门电路G2的特性极其相等的组合的单位电路存在的概率因为依存于电路的制造工艺和设计手法的因素大，所以重要的是把单位电路群中包含的单位电路数最优化。

此外，作为提高随机数的质量的其他方法，增加使用异或电路EX和触发器FF的累加的次数的方法也是有效的。具体而言，在图8所示的动作波形中，把（n+1）个单位电路的累加延长到m倍即（n+1）×m。即跨m次读出单位电路UC0~UCn的前输出D0~Dn，决定1位的随机数R（RR）。

图9表示本发明的真随机数发生电路和元素电路的一个实施例的

电路图。图9（a）所示的真随机数发生电路中，图9（b）所示的单位电路（元素电路）按M×N配置为矩阵。

一行如上述图7的电路那样连接，在输出部设置由行选择信号所选择的与非门电路G0和计时反相电路CN0。由M个构成各行的单位电路中，对应的单位电路由列解码器形成的列选择信号C0~CM-1公共地选择。上述N个行方向配置的单位电路由行解码器形成的行选择信号R0~RN-1选择一个。该行选择信号R0~RN-1作为上述与非电路G0和计时反相电路CN0构成的行选择电路的选择信号使用。构成选择电路的计时反相电路CN0在它为非工作状态时，变为输出高阻状态，所以上述N个计时反相电路的输出信号公共连接，所选择的对应于1行计时反相电路的输出信号传递给与非门电路G11。

通过由动作控制信号ACT控制栅极的与非门电路G0和反相电路INV10，时钟CLK提供给M进制计数器。据此，在M进制计数器中，当动作控制信号ACT为有效状态时，与时钟CLK对应，进行0~M-1的计数动作，由列解码器形成C0~CM-1的选择信号，单位电路的输出信号与图7的实施例相同地串行输出。

上述M进制计数器的进位信号提供给N进制计数器，所以N进制计数器与M进制计数器的1圈对应，进行计数动作。据此，如果进行配置在上述行方向的M个单位电路的读出，就进行行选择的切换，从第0行到第RN-1行，分别实施N个单位电路的读出。

在本实施例中，以M×N周期进行全部单位电路的读出，所以通过M×N周期，能从输出RR发生1位的真随机数。通过把它反复K次，能取得K位的真随机数。在本结构中，选择M×N的数，从而在M×N个单位电路中至少存在一个响应上述电信号噪声的单位电路。须指出的是，在上述K次的反复中，可以取出J个（0<J<K的整数）随机数。可是这时，各随机数位的取出周期必须分成M×N周期以上。此外，如果选择M的数，从而在由M构成的单位电路中至少存在一个发生上述真随机数的单位电路，则在每M周期（各行）能取出1位的真随机数RR，所以能构成通过M×N周期能发生N位的真随机数的真随机数发生电

路。

图9（b）表示上述图9（a）的电路元素的一个实施例的具体电路图。单位电路在上述图7的门电路G1~G4中追加用于设置行/列选择功能的门电路G5和G6。对与非门电路G5的2个输入提供列选择信号Ci和行选择信号Ri。对门电路G3，与上述图7的单位电路相同，为该行提供前1级的单位电路的输出信号Di。据此，只有行和列变为选择状态的一个单位电路变为上述的工作状态。

图9（c）表示图9（b）的电路元素的另一实施例的具体电路图。单位电路使图9（b）和上述图7所示的门电路G1~G4为3输入与非门，使其具有行/列选择功能。为与非门G5和G6的3个输入中的2个输入提供列选择信号Ci和行选择信号Ri。对门电路G7，与图9（b）和上述图7的单位电路相同，为该行提供前1级的单位电路的输出信号Di。据此，只有行和列变为选择状态的一个单位电路变为上述的工作状态。

图9（a）的计时反相电路CN如图9（d）所示，由电源电压VDD和电路的接地电位VSS之间串联的P沟道MOSFETQ1、Q2和N沟道MOSFETQ4、Q3构成。P沟道MOSFETQ1和N沟道MOSFETQ3的栅极公共连接，成为输入端子A。P沟道MOSFETQ2和N沟道MOSFETQ4的漏极公共连接，成为输出端子B。而且，从端子C提供的控制信号提供给N沟道MOSFETQ4的栅极，上述控制信号由反相电路INV12翻转，提供给P沟道MOSFETQ2的栅极。

从端子C供给的行选择信号那样的选择信号为高电平时，N沟道MOSFETQ4和P沟道MOSFETQ2变为导通状态，与接受来自输入端子A的输入信号的N沟道MOSFETQ3和P沟道MOSFETQ1的通/断对应的输出信号从输出端子B输出。从端子C供给的行选择信号那样的选择信号为高电平时，N沟道MOSFETQ4和P沟道MOSFETQ2同时变为导通状态，根据来自输入端子A的输入信号、N沟道MOSFETQ3或P沟道MOSFETQ1变为导通状态，从输出端子B输出低电平或高电平。

此外，图9（a）的计时反相电路CN是图9（e）所示的传输门电路。计时反相电路CN如图9（e）所示，由输入端子A和输出端子B之间串

联的P沟道MOSFETQ5、N沟道MOSFETQ6构成。从端子C供给的控制信号提供给N沟道MOSFETQ6的栅极，上述控制信号由反相电路INV14翻转，提供给P沟道MOSFETQ5的栅极。当从端子C供给的行选择信号那样的选择信号为高电平时，P沟道MOSFETQ5和N沟道MOSFETQ6变为导通状态，来自输入端子A的输入信号从输出端子B输出。从端子C供给的行选择信号那样的选择信号为高电平时，N沟道MOSFETQ4和P沟道MOSFETQ2同时变为导通状态，通过来自输入端子A的输入信号，N沟道MOSFETQ3或P沟道MOSFETQ1变为导通状态，从输出端子B输出低电平或高电平。此外，从端子C提供的行选择信号那样的选择信号为低电平时，N沟道MOSFETQ4和P沟道MOSFETQ2同时变为截止状态，输出端子B变为高阻。

图10表示本发明的真随机数发生电路和元素电路的另一实施例的电路图。图10（a）所示的真随机数发生电路中，图10（b）所示的单位电路按M(列)×N（行）配置为矩阵。每一行按上述图7的电路那样连接，在输出部设置与非门电路G0和异或电路EX。与非门电路G0的另一个输入与电源VDD连接，总是高电平（逻辑1）状态。由M个构成各行的单位电路中，对应的单位电路由列解码器形成的列选择信号C0~CM-1公共地选择。

通过由动作控制信号ACT控制栅极的与非门电路G0和反相电路INV10，将时钟CLK提供给M进制计数器。据此，在M进制计数器中，与图7的实施例相同，当动作控制信号ACT为有效状态时，与时钟CLK对应，进行0~M-1的计数动作，由列解码器形成C0~CM-1的选择信号，由N行构成的共用Ci的各行单位电路的输出信号，串行输出。

与非电路G0的输出与异或电路EX0的一个输入连接。异或电路EX0的输出与相邻行的异或电路连接，全部行的异或电路的输出依次与相邻的行串联。对异或电路EX0的另一个输入，虽然未特别限定，但是提供高电平（逻辑1）那样的固定值。据此，如果从所选择的共用Ci的N行单位电路中发生的N个数出信号的任意一个变化，与它对应，各行的异或电路的各输出信号变化，通过上述串联的异或电路，

串联的异或电路的输出信号RA变化。即上述输出信号RA变为用1周期的动作反映N个单位电路（基本电路）的电噪声的值。

在本实施例中，在M周期中进行全部单位电路的读出，所以通过M周期，能从输出RR发生1位的真随机数。通过把上述过程反复K次，能取得K位的真随机数。在该结构中，选择M×N的数，从而在M×N个单位电路中至少存在一个响应上述电信号噪声的单位电路。须指出的是，在上述K次的反复中，可以取出J个（0<J<K的整数）随机数。可是这时，各随机数位的取出周期必须分开M周期以上。

图10（b）表示上述图10（a）的真随机数发生电路的电路元素的一个实施例的具体电路图。对与非门电路G1和G2的2个输入的一个提供列选择信号Ci。对门电路G3，与上述图7的单位电路相同，提供该行前1级的单位电路的输出信号Di。据此，只有列变为选择状态的一个单位电路变为上述的工作状态。

图11表示用于说明图9的真随机数发生电路的动作的一个例子的概略波形图。当动作控制信号ACT为高电平的有效电平状态时，如果输入时钟CLK，则与它对应，列选择信号C0~CM-1从列解码器输出。这时，N进制计数器因为计数值为0，所以使第0行的行选择信号R0为选择电平，所以第0行的单位电路的输出信号与列选择信号C0~CM-1对应，串行输出。如果进行第0行的单位电路的读出，则根据进位信号，N进制计数器进行+1的计数动作，使上述第0行R0为非选择，而使第一行R1为选择状态。依次进行到N-1行的单位电路的读出。真随机数RR由上述单位电路的串行输出R、与前1个输出的异或决定。须指出的是，图10的真随机数发生电路的动作波形图与图9类似，所以省略。与图9的不同点在于没有选择信号R0~RN-1。据此，不需要用于进行N进制计数器的动作，因此，全部选择M×N个单位电路（基本电路）所需要的周期变为M次。

图12表示本发明的真随机数发生电路的另一实施例的概念图。在本实施例中，通过组合算术方式的随机数发生电路、利用本发明的物理现象的真随机数发生电路的方法，发生随机数。如上所述，算术方

式的随机数发生电路中，虽然电路规模比较小，但是取得的随机数的质量不高。当取得无数的随机数时，存在表现周期性的本质的缺点。因此，在算术方式的算法中，把本发明的真随机数发生电路中响应电信号噪声的不规则的元素作为初始值插入，可降低周期性。

图13表示图12的初始值发生电路的一个实施例的电路图。基本上本实施例与上述图6的实施例相同。不同点在于代替异或电路EX0~Exn，设置触发器FF0~FFn，从该触发器FF0~FFn取得D0~Dn那样的初始值。

上述信号D0~Dn中的大部分由于上述工艺离差，而变为固定值，但是其中任意1位～数位成为响应电信号噪声的随机数，所以能充分发挥作为上述算术方式的随机数发生电路的初始值的功能。

图14表示图12初始值发生电路的另一个实施例的电路图。本实施例与上述图6的实施例基本相同。不同点在于通过使信号ACT有效，从触发器FF输出1位随机数。即在本实施例中，把1位随机数作为上述算术方式的随机数发生电路的初始值使用。

图15表示用于说明图13和图14的初始值发生电路的动作的波形图。如果动作控制信号ACT变为高电平，在图13的电路中，从单位电路UC0~UCn中，输出输出信号R0~Rn。输出信号R0~Rn如上所述，存在成为固定值的、与电信号噪声对应变化的信号。如果动作控制信号ACT从高电平变为低电平，此时与上述输出信号R0~Rn对应的随机数D0~Dn由触发器FF0~FFn取入，输出由包含固定值的D0~Dn构成的多位随机数。

在图4的电路中，上述各单位电路UC0~UCn的输出信号R0~Rn提供给异或电路EX0~EXn，与这时的信号R0~Rn对应的1位随机数通过异或电路EX0~Exn输出。因此，如果动作控制信号ACT从高电平变为低电平，这时发生的随机数由触发器FF0~FFn取入，输出由1位构成的随机数DM。

图16表示本发明的真随机数发生电路的另一实施例的电路图。本实施例在上述图9所示的真随机数发生电路中设置输出识别信息F的

输出端子。即从M×N个单位电路输出的M×N个数出信号作为识别信息F输出。上述识别信息F保持到适当的存储电路中，登记到管理系统中。作为识别信息F的比对方法，除了登记时和比对时的环境和条件的不同，如上所述，还需要允许响应电信号噪声的真随机数所对应的识别编号的变动。把对装有上述真随机数发生电路的半导体集成电路器件接通电源时或者使上述动作有效信号ACT有效之后的识别信号F存储到适当的存储电路中，将其作为被识别编号。从管理系统依次取出登记识别编号。比较登记识别编号和被识别编号。

登记识别编号和被识别编号的比较结果差异、以小的那个作为一致候选。反复对管理系统登记的登记识别编号的动作，最终全部登记识别编号中差异最小的成为相同最有力候选。

在比较登记识别编号和被识别编号时，对应的位的“0”、“1”的输出图案是各登记识别编号特有的，用构成图案的位数的一致的比例就能判断是否是从相同半导体集成电路器件输出的识别编号。允许登记时和比对时的环境或上述随机数位中的不同引起的识别编号的变动，所以通过把被识别编号和识别完毕的识别编号的离差合计最小的作为一致的候选，从而能识别芯片。

图17表示本发明的真随机数发生电路的一个实施例的电路图。该实施例的基本结构与上述图9的实施例相同。在本发明中，利用如果着眼于MOSFET的特性离差是随机的分布，观察多个单位电路，则第一反相电路INV1和第二反相电路INV2或第一门电路G1和第二门电路G2的特性极其相等的组合以一定概率存在。因此，当在半导体集成电路器件中制造真随机数发生电路时，检查是否实际存在反映电信号噪声的单位电路是不可欠缺的。

在本实施例中，在真随机数发生电路中附加检验自身的测试电路。测试电路中的检查方法是判断单位电路群中包含的第一门电路G1（第一反相电路INV1）和第二门电路G2（第二反相电路INV2）的特性极其相等的组合的单位电路的数量，保证可靠地捕捉到基于物理现象的电信号噪声。

如在上述图16中取出识别信息F那样，把取得来自各单位电路的输出信号的电路节点即反相电路INV11的输出端子（异或电路EX的一个输入）的信号R提供给反相检测器，由计数器对检测信号H计数。该计数输出C在比较器中进行比较，得到判断结果M。此外，为了上述测试动作，由（4+M）进制计数器形成列选择信号。（4+M）进制计数器如果连续4次选择相同的单位电路，就反复进行转移到下一单位电路的选择动作的工作。

图18表示用于说明上述测试电路的动作一个例子的时序。使测试信号TS为高电平，指示（4+M）进制计数器动作。此外，使反相检测器和计数器为初始状态或初始值。使动作控制信号ACT为高电平，使随机数发生电路为工作状态。提供时钟CLK，进行从最初的单位电路开始的依次的读出动作。这时，（4+M）进制计数器对于时钟CLK1~4，连续4次选择相同的单位电路。据此，如上述图2（b）所示，输出固定值的4次都输出相同的信号R。

这样输出固定值时，反相检测器不进行反相检测，计数器的计数值不增加。而如图2（a）所示，如果存在形成响应电信号噪声Vnz的输出信号R，则4次访问中的翻转次数最大为3次，1次以上的翻转时，检测结果为真。在相同图中，第二周期和第四周期中输出信号R变化，在反相检测器中，输出H的电平每次变化。

如果输出H变化1次，当结果为真时，使计数器的值C0从低电平变化为高电平，计数值增加1。转移到单位电路群中的下一单位电路的选择，反复进行与上述相同的检测动作，直到最后的单位电路。当计数器的数比规定值大时，检测结果M的值为真（高电平）。当取得真随机数时，基本上上述规定值为1就可以，但是考虑稳定性，优选地是2或3以上的数。

如图18所示，当计数器为2位输出的二进制计数器时，比较器在时钟CLK的第K-1周期检测到计数输出C0和C1都变为高电平，如果上述检查结果M决定为高电平，则如图2（a）所示，确定形成响应电信号噪声Vnz的输出信号R存在4个以上。

检查一个单位电路时，虽然用4个CLK脉冲访问4次，但是只要访问大于等于2次即可。访问2次时，使用（2+M）进制计数器。在检查以外时，上述测试信号TS对应为低电平，如上所述，作为M进制计数器工作。或者，原封不动作为（4+M）进制计数器或（2+M）进制计数器工作。这时，读出周期增加为4倍或2倍。

作为安全产品的政府机关的规定，有NIST（美国标准技术研究所）决定的FIPS140-2。其中，规定了政府的购入品具有的加密模块应该的满足的安全要件（FIPS PUB140-2，SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES），关于随机数，表示基于统计手法的质量检测合格标准。在使用该方法的方法中，存在用于实现它的专用电路的规模比较大、用半导体检测器件检查时比较花费时间的缺点。

而在本发明的随机数发生电路中设置的测试电路中，在半导体晶原上完成电路的时刻，不用与具有上述测试功能的测试器连接，就能自己进行判断。此外，作为半导体集成电路器件，在出厂时，也能自己进行判断。如果必要，在装到系统的时刻，可以按照需要，或者定期确认上述真随机数发生电路是否是能正常工作的状态。据此，可靠性高的真随机数发生成为可能。本方式由统计保证，从而是可能的。

真随机数发生电路的诊断（检测）等于随机数的质量的评价，需要一定统计上的处理。因此，存在检测器件、检测时间、长期可靠度保证等大的课题。把真随机数发生器装到LSI和最终系统中后，电路自身是否正常工作是重要的问题。这是因为如果不能取得质量高的真随机数，就会危及安全。可是，检测或监视真随机数发生电路对工作中的系统而言，是大负载。对于这样的技术课题，本发明的真随机数发生电路中，如上所述，用简单的结构就能解决这些问题。

图19表示本发明的真随机数发生电路的一个实施例的电路图。本实施例的基本结构与图9的实施例相同。在本实施例中，作为时钟，使用由振荡器形成的振荡脉冲OSC。

图20表示图19的真随机数发生电路的动作波形图。通过有效信号

ACT，振荡器发生特定周期Tosc的脉冲。接收脉冲OSC，依次选择单位电路群中的单位电路，在RR信号中发生随机数。如果开始信号ST变为高电平，就从输出RY取出RR信号的随机数。开始信号ST的周期Tc和振荡器的周期Tosc的关系因为需要读出来自全部单位电路的输出信号，所以是[Tc]≧[Tosc]×[n]。这里，上述“n”是单位电路群中的单位电路数（M×N）。振荡器输出脉冲OSC可以是装有该真随机数发生电路的LSI的系统时钟等。

图21表示本发明的真随机数发生电路的一个实施例的电路图。本实施例的基本结构与图19的实施例相同。在本实施例中，省略开始信号ST，根据动作控制信号ACT，变为工作状态，在输出之前设置移位寄存器，发生由并列位构成的随机数RAi。

图22表示本发明的真随机数发生电路的输出部的另一个实施例的电路图。本实施例把上述图21的实施例的移位寄存器变更为存储器。图22中使用的存储器是所谓的串行输入/并行输出类型的存储器。控制信号ACT为高电平时，从真随机数发生电路，在时钟的每M×N周期，从RR 每次发生1位真随机数，同时该存储器是串行输入模式，从输入SI取入真随机数，存储。控制信号为低电平时，真随机数发生电路停止，同时该存储器为并行输出模式，从输出DT输出与输入AD的地址信息对应的存储器空间中存储的真随机数。须指出的是，该存储器的各输入输出的意思为，SE是用于切换存储器的模式的控制输入，高电平时为串行输入模式，低电平时为并行输出模式，SI是串行数据输入，CK是取入串行输入时的同步信号输入，AD是选择并行输出模式时存储器空间的地址输入，DT是并行数据输出。

图22所示的存储器可以是FIFO（First In First Out先入先出）型存储器、能同时进行串行输入和并行输出的非同步型存储器。

图23表示上述图21所示的真随机数发生电路的动作波形图。通过动作控制信号ACT，电路变为工作状态，通过N进制计数器的进位信号CA，移位寄存器进行1位的移动动作，进行发生的真随机数RR的取入。在该实施例中，通过0到7构成的8次前一个单位电路群的读出，

能并行输出由8位构成的随机数D0~D7。

图24表示本发明的真随机数发生电路的一个实施例的芯片结构图。在本实施例中，由一个IC构成真随机数发生电路。作为外部端子，由电源端子VCC、VSS、时钟输入端子CLK、动作控制信号RST以及真随机数输出端子RR构成。如上所述，在装有振荡器的电路中，省略时钟端子CLK。此外，在具有测试电路的电路中，附加判断输出端子、测试模式输入端子。判断输出端子能共用为随机数输出端子RR。可以这样的IC芯片密封在一个封装中，可以装到与其它IC相同的安装衬底上，密封（多芯片IC），此外，可以原封不动安装到系统中。

图25表示本发明的半导体集成电路器件的一个实施例的框图。本实施例的各电路模块按照实际的半导体衬底上的几何学的电路配置描绘。本实施例的半导体集成电路器件虽未特别限制，但是是组合多个电路功能块，并具有特定的信号处理功能的半导体集成电路器件。在具有这样的电路模块的半导体集成电路器件中装载真随机数发生电路。真随机数发生电路所需要的时钟，使用该半导体集成电路器件中设置的时钟发生电路形成的时钟，或者接受从外部端子提供的时钟并使用该时钟。此外，如图19和图21的真随机数发生电路那样，在具有振荡器的电路中，不需要提供上述时钟。

图26表示本发明的半导体集成电路器件的另一个实施例的框图。本实施例的各电路模块也按照实际的半导体衬底上的几何学的电路配置描绘。本实施例面向以MPU（微处理器）为中心的单片微型计算机。在该微型计算机中，在总线BUS（地址总线、数据总线和控制总线）上，除了上述MPU，还连接RAM（随机存储器）、ROM（只读存储器）、DMAC（直接存储器访问控制器）、TIM（定时器）、ADC（模拟数字控制器）、DAC（数字模拟转换器）、上述真随机数发生电路。

本发明的真随机数发生电路全部只由标准CMOS逻辑电路实现。这能减轻复杂的模拟电路设计和LSI安装所需的工作，降低产品的价格，有助于提高可靠性。此外，针对作为安全问题上最大的课题的开裂，能提供牢固的模块。这是因为通过只用标准逻辑电路构成，能取

得在LSI中从攻击的目标逃脱的迷彩（隐形）效果。使用模拟电路时，在电路图案中没有特征，而其如上所述，通过总线BUS取出随机数时，能进一步提高上述的迷彩（隐形）效果。

图27表示本发明的真随机数发生电路的另一实施例的结构图。图27（a）表示电路模块结构，图27（b）表示布局结构。在本实施例中，设置n个图7所示的真随机数发生电路。即设置0~n-1构成的n个真随机数发生电路，各自的输出信号R0、R1~Rn-1通过多路复用器MUX，选择一个信号，作为真随机数RM输出。

如图27（b）的布局结构所示，通过夹着多路复用器，在其上下设置真随机数发生电路，能高效地进行电路配置。在相同图中，真随机数发生电路中的一个电路模块表示上述一个单位电路。在该结构中，由2个真随机数发生电路夹着的多路复用器可以是二选一那样的比较简单的结构，所以在配置多路复用器的部分配置上述解码其等选择信号发生电路。

在本实施例的真随机数发生电路中，为了取得随机数R而由n个单位电路构成时，为了取得1位随机数R，需要得到来自全部单位电路的输出信号，所以需要n个周期。因此，与取得上述一个随机数所需要的n个周期对应，如本实施例那样设置n个随机数发生电路时，能以与时钟CLK同步的高频率发生随机数。但是，通过动作控制信号开始动作时，需要由n个周期构成的虚拟周期。

图28表示图27所示的真随机数发生电路的动作一例的时序图。图27的真随机数发生电路中，为了最初的随机数发生电路的读出，n周期（n时钟）后，从各真随机数发生电路输出随机数R0~Rn-1，所以通过多路复用器MPX，与时钟CLK同步，每次选择一个，从而如与时钟CLK同步的真随机数RM（R0、R1、R2、…、Rn-1、R0’、R1’、R2’…）那样，取得与时钟CLK同步的高比特率的真随机数。

图29表示应用本发明的IC卡的一个实施例的外观图。IC卡具有塑料盒构成的卡101、装在该卡101的内部的未图示的单片微型计算机构成的IC卡用芯片。上述IC卡具有连接在上述IC卡用芯片的外部端子上

的多个接点（电极）102。

多个接点102是后面根据图30说明的电源端子VCC、电源基准电位端子VSS、复位输入端子$\overline{RES}$、时钟端子CLK、数据端子I/O-1/$\overline{IRQ1}$、I/O-2/$\overline{IRQ2}$。IC卡通过该接点102从未图示的读写器那样的外部结合器件接受电源供给，与外部结合器件之间进行数据通信。

图30表示本发明的装在IC卡上的IC卡用芯片（微型计算机）的一个实施例的概略框图。图30的各电路模块通过公开的MOS集成电路的制造技术，未特别限制，但是形成于单晶硅那样的一个半导体衬底上。

本发明的IC卡用芯片的结构基本上是与微型计算机相同的结构。该结构由时钟发生电路、中央处理器件（以下称作CPU）、ROM（Read Only memory）、RAM（Random Access Memory）、非易失性存储器（EEPROM）等存储器件、进行加密和解码处理的计算的协处理器（加密和解码器件）、输入输出端口（I/O端口）构成。

时钟发生电路是接受从未图示的读写器（外部结合器件）通过图29的接点102供给的外部时钟，形成与该外部时钟信号同步的系统时钟信号，把它提供给芯片内部的电路。

CPU是进行逻辑运算和算术运算的器件，控制系统控制逻辑、随机数发生器和安全逻辑以及定时器。RAM、ROM、EEPROM等存储器件是存储程序和数据的器件。协处理器由适合于DES加密法的电路构成。I/O（输入输出）端口是与读写器进行通信的器件。数据总线和地址总线是相互连接各器件的总线。

上述存储器件中的ROM是存储内容非易失去的固定存储器，主要是存储程序的存储器。易失性存储器（以下称作RAM）是能自由置换存储信息的存储器，但是如果中断电源的供给，存储的内容就消失。如果从读写器拔出IC卡，电源的供给中断，所以上述RAM的内容不保持。

上述非易失性存储器（以下称作EEPROM（Electrical Erasable Programmable Read Only Memory）是能进行内容的改写的非易失性存储器，其中的信息一旦写入即使电源的供给停止，也能保存在其内部。

EEPROM用于存储时，需要进行改写，并且即使从读写器拔出IC卡，也应该保存全部被存入的数据。例如把IC卡作为预付卡使用时，在每次使用时改写预付的度数等。这时的度数，即使从读写器拔出，也需要存储保持，所以用EEPROM保持。

CPU采用与所谓的微处理器相同的结构。虽然未图示细节，但是在其内部具有命令寄存器、把写入命令寄存器的命令译码并且形成各种微处理器命令和控制信号的微处理器命令ROM、运算电路、通用寄存器（RG6）、与内部总线BUS结合的总线驱动器、总线接收器等输入输出电路。CPU读出ROM中存储的命令，进行与该命令对应的动作。CPU进行如下控制：通过I/O端口输入的外部数据的取入、来自ROM的命令或命令的执行所需要的固定数据的读出、对于RAM和EEPROM的数据写入和读出动作。

上述CPU接受从时钟发生电路发生的系统时钟信号，按照根据系统时钟信号决定的动作时序、周期进行工作。CPU内部的主要部分由P沟道MOSFET和N沟道MOSFET构成的CMOS电路构成。虽然未特别限制，但是CPU包含CMOS静态触发器那样的可静态工作的CMOS静态电路，和将对信号输出节点的预充电和对信号输出节点的信号输出、与系统时钟信号同步进行的CMOS动态电路。

协处理器在内部处理的普通数据上附加符号位，使其具有正/反两方的状态。在加密的反复运算时，按各符号随机变更数据。不受符号的影响的运算（异或）忽略符号，进行运算。在受符号的影响的运算（使用变换表的运算）中，准备用于正的运算电路和用于负的运算电路，根据数据的符号，选择运算电路的输出。

DES（Data Encryption Standard）是广泛使用的密钥模块加密。DES的算法大致能分割为普通数据流和密钥的数据流。在普通数据流中，进行成为IP的转置后（信号的改变）后，按高位和低位各32位分割数据，反复16次转置和换字处理。最后把高位和低位各32位数据合并，进行称作IP^{-1}的转置，取得加密文。

在DES中，能用相同的处理实现加密和解码。可是，在加密和解

码中，密钥的调度不同。关于密钥的调度部分，虽然省略了细节，但是根据密钥数据，对各段进行48位密钥调度数据的输出。

在DES算法中，对于相同的普通文，总进行相同的内部动作。结果，内部信号依存与输入信号变化，所以容易进行用DPA（Differential Power Analysis）法的统计处理。即在DPA法中，统计处理功耗电流波形，推测密钥，例如应用假定为DES的某部分的密钥，一边使普通文变化，一边测定功耗电流波形，统计。一边使密钥进行各种变化，一边反复该作业，当正确的密钥时，电流波形表现大的峰值。

作为基于上述DPA的对于DES解码的对策的例子，有特开2000-066585号公报。在该公报中记载的技术中，设置掩码a的图案、位翻转的掩码图案对，每次进行加密时，通过开关选择该对的一方，屏蔽依存于器件内部的普通文的位，输出加密文之前，从加密文除去掩码a的影响。

虽然已经说明了为了防止基于DPA的解码，需要上述掩码不偏向于特定的图案，但是为了无论怎样，对多位的图案都不偏向，利用由随机数发生器发生的随机数。

图31表示应用本发明的非接触IC卡的一个实施例的框图。对于非接触IC卡，也设置作为外部器件而设置的读写器件的线圈（天线）。装在非接触IC卡上的LSI除了图示的模块，还设置存储器和微型计算机等功能块，但是把它们表示为逻辑电路和非易失性存储器。构成上述LSI的各模块的电路元件虽然未特别限制，但是通过公开的MOSFET（金属氧化物半导体场效应晶体管。在本说明书中，为MOSFET，为绝缘栅类型场效应晶体管的总称）集成电路的制造技术，形成于单晶硅的一个半导体衬底面上。此外，LSI由给定的保护膜进行积层处理后，装在成为非接触IC卡的基体的卡面上，进行保护膜处理。

本实施例的非接触IC卡虽然未特别限制，但是为所谓的紧贴类型的非接触IC卡，具有使用铜箔在卡面上形成线圈状的受电线圈（卡一侧天线）、通过给定的布线层与上述受电线圈结合的LSI。LSI通过4个

二极管桥接而成的整流电路、使整流电路的整流电压平滑的平滑电容器、稳定化电源电路，形成包含上述逻辑电路和非易失性存储器的内部电路的工作电压VDD。对于上述整流电路，实质上并列设置时钟发生电路、数据接收电路和数据发送电路。

由上述二极管桥路构成的整流电路通过与读写器件的发送线圈（天线）的电磁耦合，把作为电源传递给非接触IC卡受电线圈的交流信号、即载波进行整流，把由上述平滑电容器平滑的电压通过稳压源发生直流电源电压VDD，作为工作电源提供给LSI的各功能块。电源接通复位电路检测电源电压VDD的上升，即检测与读写器件的结合，为了正常进行数据的收发，把逻辑电路的寄存器和锁存电路复位。

数据接收电路利用调频载波、接收、解调从读写器件而传送的数据，作为内部输入数据传递给LSI的内部电路。内部电路中形成的输出数据通过数据发送电路，将载波调频，并传送给读写器件。

上述内部电路(逻辑电路)和数据接收电路以及数据发送电路中，除了上述工作电压VDD，为了动作序列控制和信号的收发，还需要时钟信号。在本实施例中，通过时钟发生电路，使上述交流信号变为脉冲信号，发生时钟信号。在逻辑电路部设置随机数发生器，使用与外部的数据发送和数据接收有关的随机数。

在上述非接触IC卡中，直流电源电压VDD的电流供给能力小，所以需要随机数发生器的耗电也小。上述随机数发生器因为是使单位电路依次工作，所以能减小耗电。因此，本实施例的随机数发生器适合装在上述非接触IC上。

图32表示本发明的随机数发生电路发生的随机数的随机数2维分布图。在图32中，与点的白和黑对应，表示200×200位的随机数的0和1。虽然未特别限制，但是在本实施例中，设置128个单位电路（基本电路），用通常的CMOS工艺构成电路。

图32鉴于图面生成的原因，是以400dpi用扫描仪读取显示随机数2维分布的图，所以与实际的随机数2维分布图有若干不同，但是，表示随机数2维分布，不存在特有的图案。即表示是高质量的随机数。

此外，用上述FIPS140-2的随机数检测结果如下所述。1次检测中使用的随机数的长度为20，000位，把它进行600次的结果，全部能通过该检测。

现在加密和安全之所以成为日常的话题是因为因特网的普及。因特网是连接远离的设备的技术。在因特网上往来的数据本质上通过第三者拥有的计算机和网络设备，所以总担心窃听和篡改。为了使因特网变为能保证安全和隐私的基础结构，加密和认证引人注目。现在、在因特网上，虽然利用了各种安全技术，但是代表性的技术有SSL（Secure Socket Layer）和IPsec（Internet Procotol security）技术。虽然不描述这些技术的细节，但是都需要高质量的随机数。IPsec在下一代的因特网技术即IPv6(Internet Procotol Version6)中作为必要条件而采用。如果IPv6普及，则以个人拥有的个人电脑和移动电话为首，对汽车和家电也能分配IP编号。就需要在这些设备中容易发生质量高的随机数即真随机数。

如上所述，本发明的真随机数发生电路全部只由标准CMOS逻辑电路实现。这能减轻复杂的模拟电路设计和LSI安装所需的负载，降低产品的价格，有助于提高可靠性。

图34表示本发明的装在半导体集成电路器件中的真随机数发生电路的图1所示的基本概念的应用概念的电路图。在图1中，真随机数是多个构成的各基本电路内的INV1和INV2中发生的电信号噪声，但是在图34中，第一反相电路INV1为公共的，第二反相电路分散到各基本电路中。即只存在1种第一反相电路的逻辑阈值VLT1和各基本电路中的第二反相电路的逻辑阈值VLT2的差极小的组合存在时，能反映第一反相电路和第二反相电路的电信号噪声的影响，取得真随机数。须指出的是，第三反相电路以后的动作与上述图1上述的内容相同，所以省略。

图35表示本发明的装在半导体集成电路器件中的真随机数发生电路的图34所示的应用基本概念的另一应用概念的电路图。在本实施例中，上述图34的反相电路INV1~INV14替换为2输入的与非（NAND）

门电路G1~G14。上述门电路G1中，一个输入和输出结合。门电路G1的公共化的输入输出与基本电路内的门电路G02的一个输入连接。门电路G02的输出与门电路G03的一个输入连接。门电路G03的输出与门电路G04的一个输入连接。而且，门电路G02~G04的另一个输入与电源VDD相连，并总为高电平（逻辑1）。

图34的反相电路INV1~INV14能视为上述与非门电路G1~G14那样的逻辑门电路的一种。即进行使输入信号翻转的逻辑动作。如图34所示，使用反相电路INV1~INV4时，反相电路INV1和INV02，在初级一侧，在逻辑阈值电压VLT附近工作，在电源电压VDD和电路的接地电位之间，流过直流电流。在本发明中，如上所述，利用元件的工艺离差引起的逻辑阈值电压的正态分布，因此，需要使较多的单位电路工作，所以上述反相电路INV1和INV02中的直流电流在实现低功耗上可以忽略。

而如本实施例那样使用门电路G1~G14时，各门电路G1~G14在动作控制信号ACT为低电平（逻辑0）那样的无效电平时，门电路G1的输出无条件地变为高电平（逻辑1），以门电路G1的输出为输入的门电路G02的输出无条件地变为低电平（逻辑0），以门电路G02的输出为输入的门电路G03的输出无条件地变为高电平（逻辑1），以门电路G03的输出为输入的门电路G04的输出无条件地变为高电平（逻辑1），在各门电路G01、G02、G03、G04以及与它等价的其他基本电路内的门电路中也不发生直流电流。即在本实施例电路中，在需要随机数的时刻上，把上述动作控制信号ACT变为高电平（逻辑1）那样的有效电平。据此，各门电路G1~G14进行响应与上述动作控制信号ACT不同的另一个输入信号，形成翻转信号那样的反相电路动作。据此，通过使上述动作控制信号ACT为高电平，进行与图34的基本电路图相同的动作。

以上，根据实施例，具体说明本发明人取得的发明，但是本发明并不局限于上述实施例，在不脱离其宗旨的范围中当然能进行各种变更。例如，当电阻元件作为对于构成反相电路和门电路的信号输入

MOSFET的负载元件时，与特性离差对应的信息反映电阻元件的特性离差和信号输入MOSFET的特性离差。与电阻离差对应的特定信息没必要一定只在半导体集成电路器件内形成，也能采用通过外部端子连接的结构。可是，在实现低功耗上，优选地使用上述的CMOS门电路。此外，第一反相电路INV1和第二反相电路INV2为了降低耗电电流，替换为上述图10（b）所示的计时反相电路CN，通过动作控制信号使之有效。

工业可利用性

本发明可以在内置于网络设备、无线电通信设备、加密和复合器件、以及认证系统的随机数发生方法和半导体集成电路器件中广泛利用；也可以在内置于玩具类的机器人和游戏人物的“个性因子”和“反复无常因子”的随机数的随机数发生方法中广泛利用，或在执行内置于玩具类的机器人和游戏的人物“个性因子”和“反复无常因子”的随机数的随机数发生方法的半导体集成电路器件中广泛利用。

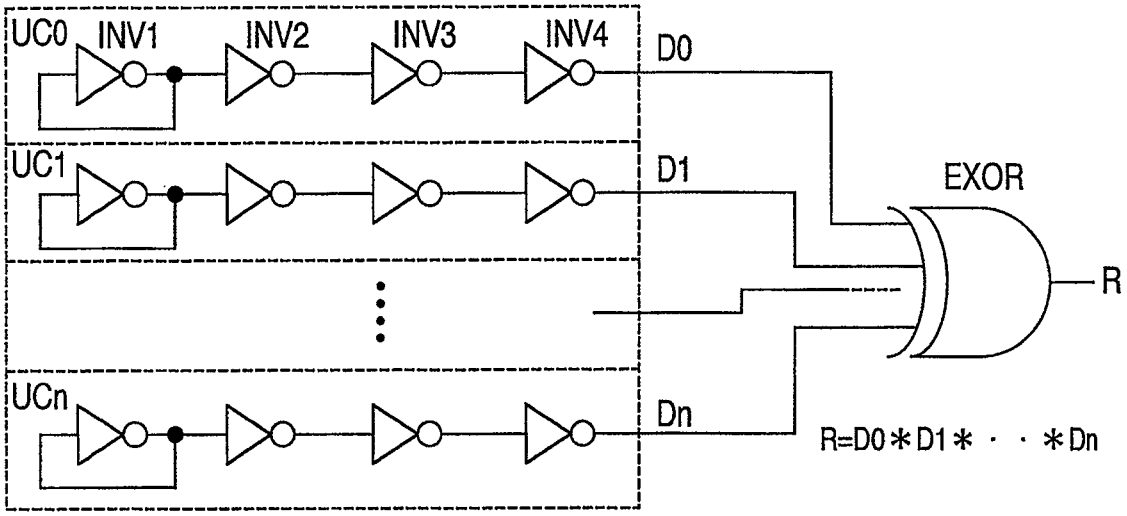


图 1

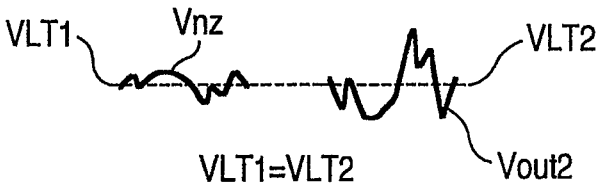


图 2（a）

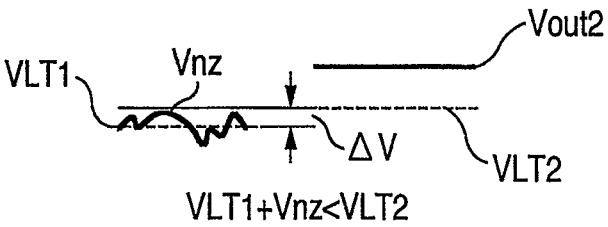


图 2（b）

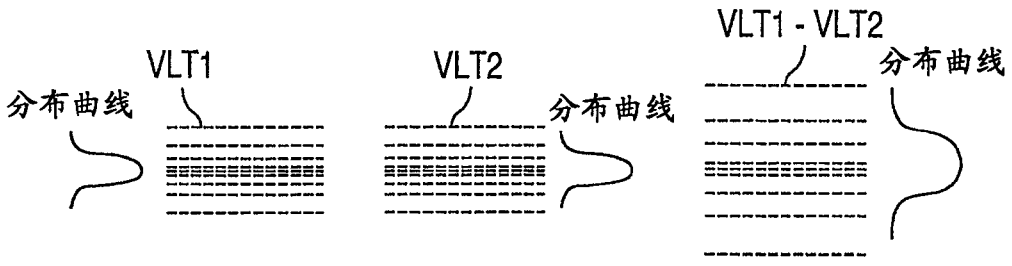


图 2（c）

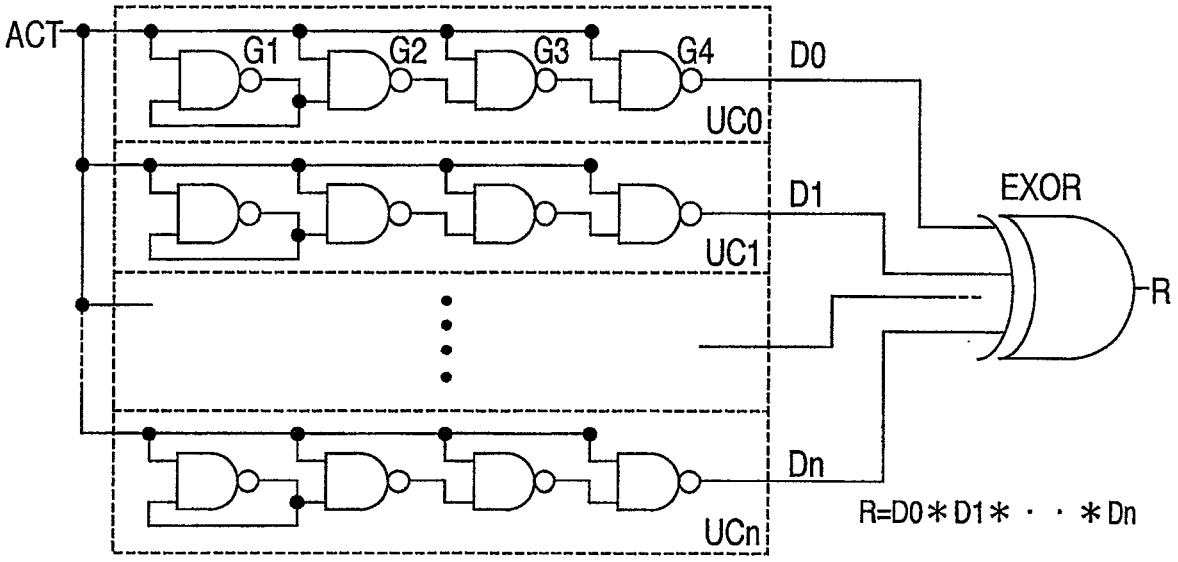

ACT
G1
G2
G3
G4
D0
UC0
D1
UC1
EXOR
R
Dn
UCn
R=D0＊D1＊・・＊Dn

图 3

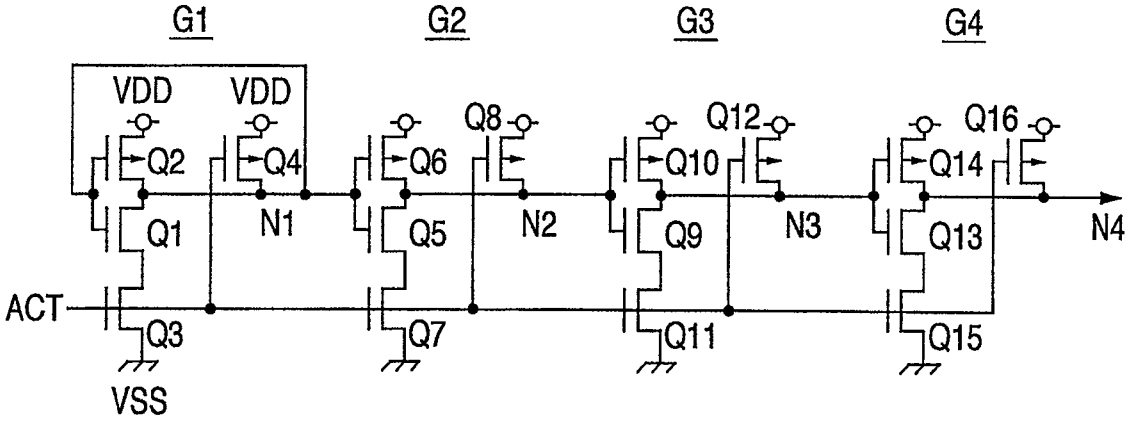

G1
G2
G3
G4
VDD
VDD
Q2
Q4
Q6
Q8
Q10
Q12
Q14
Q16
Q1
N1
Q5
N2
Q9
N3
Q13
N4
ACT
Q3
Q7
Q11
Q15
VSS

图 4

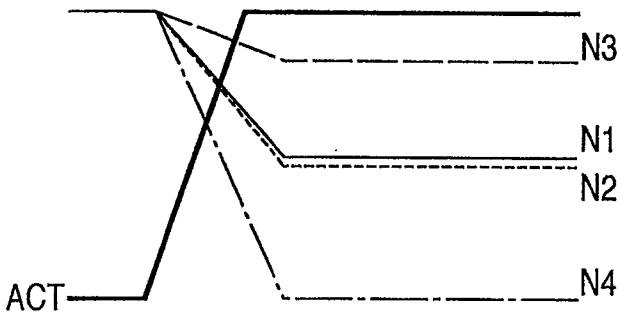

N3
N1
N2
ACT
N4

图 5

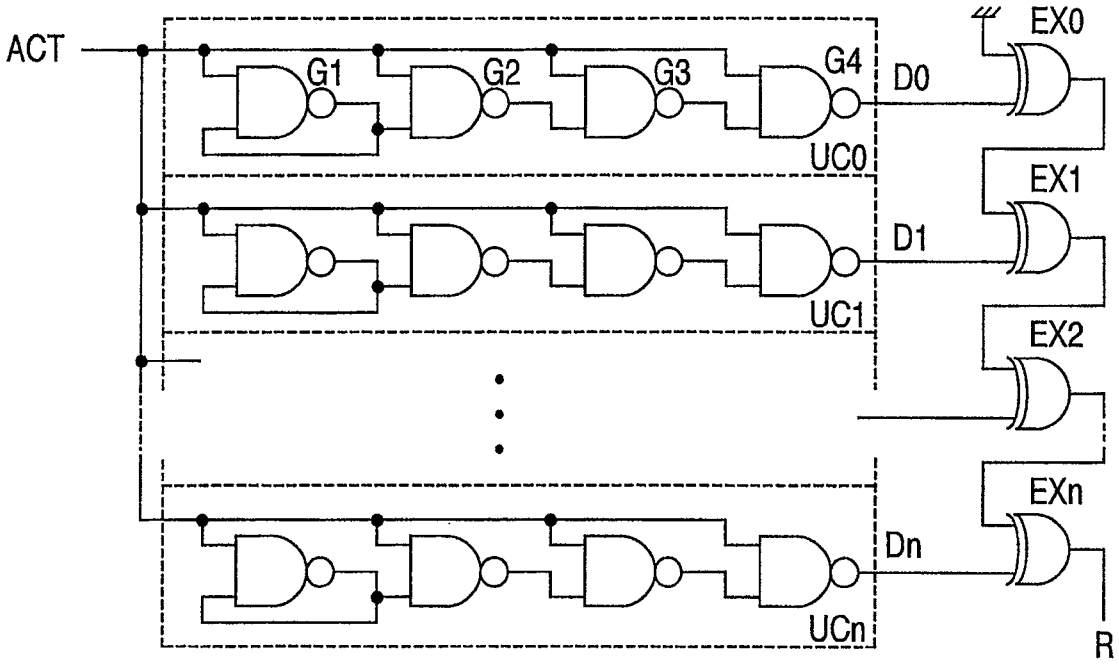

ACT
G1
G2
G3
G4
D0
UC0
EX0
EX1
D1
UC1
EX2
EXn
Dn
UCn
R

图 6

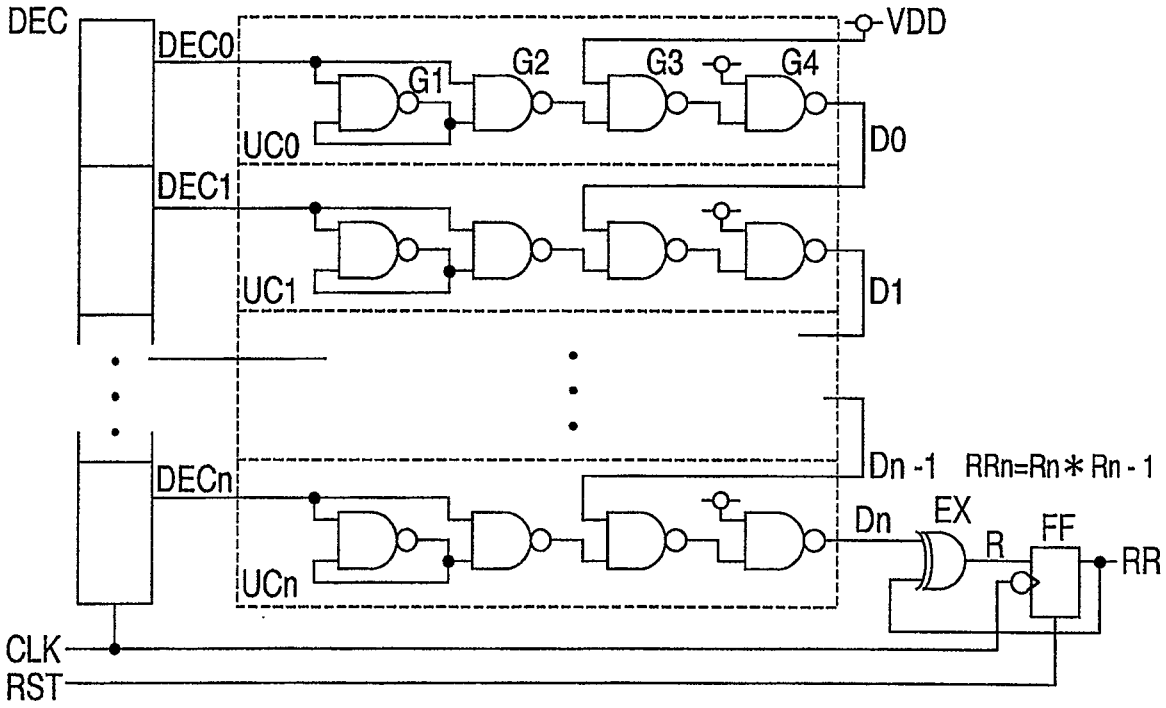

DEC
DEC0
DEC1
DECn
VDD
G1
G2
G3
G4
UC0
UC1
UCn
D0
D1
Dn -1
RRn=Rn＊Rn - 1
Dn
EX
R
FF
RR
CLK
RST

图 7

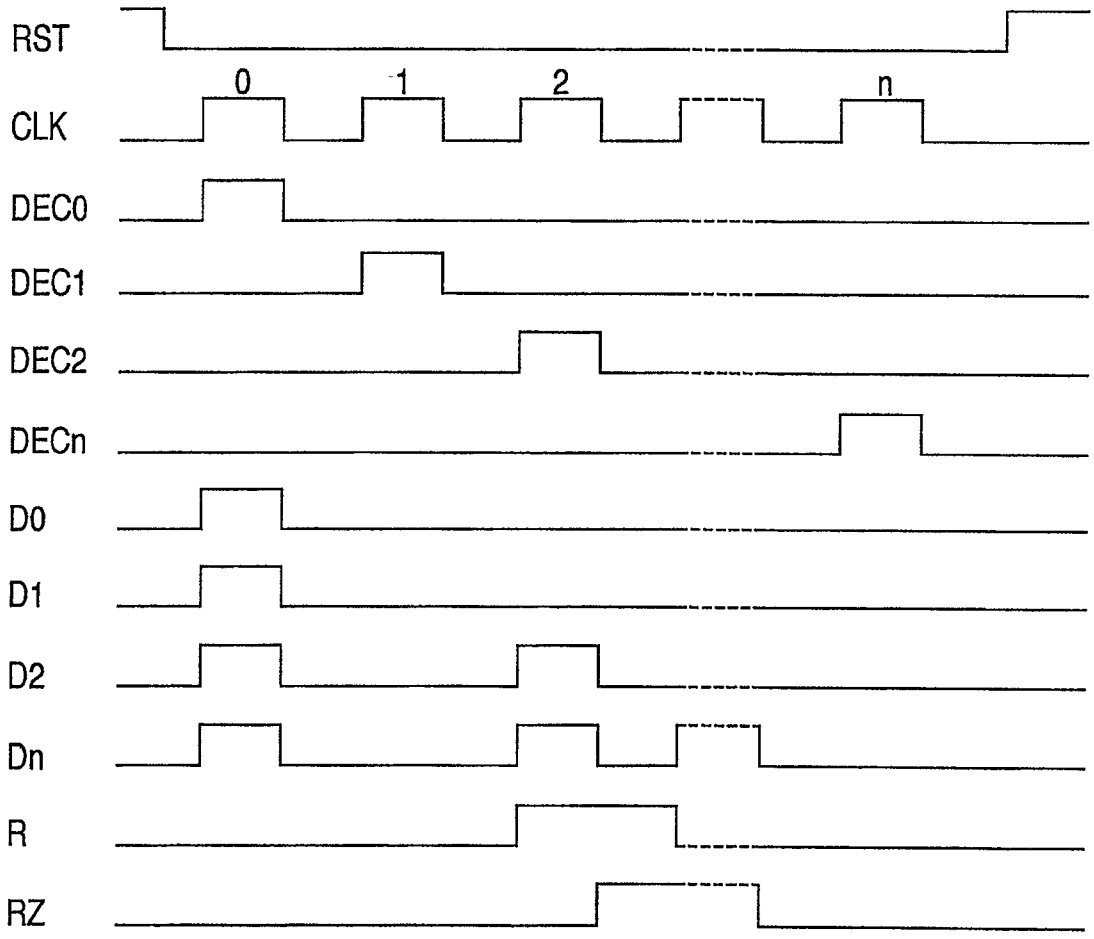


图 8

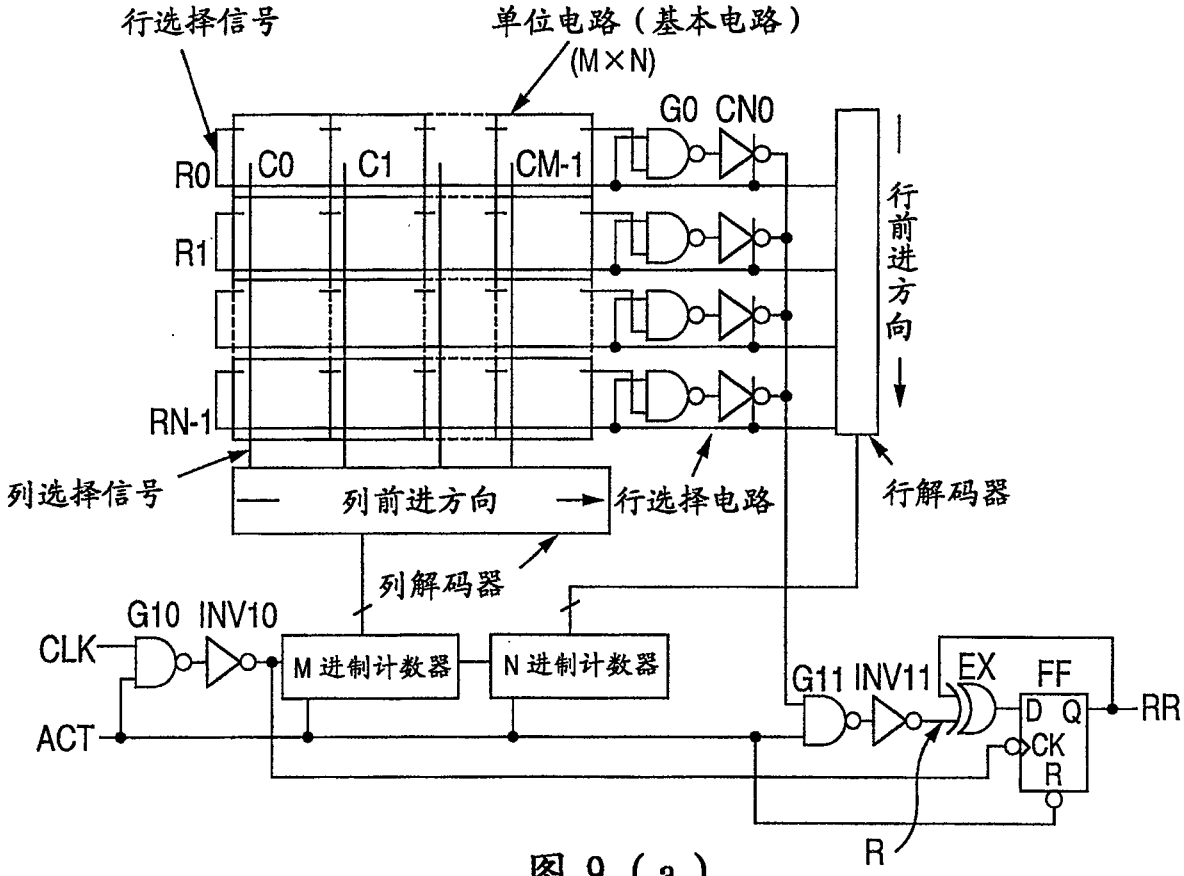


图 9（a）

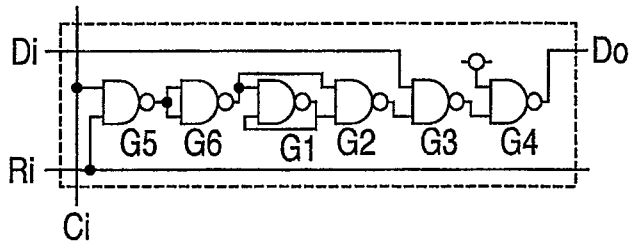


图 9（b）

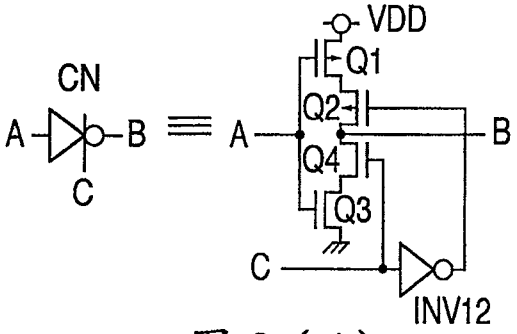


图 9（d）

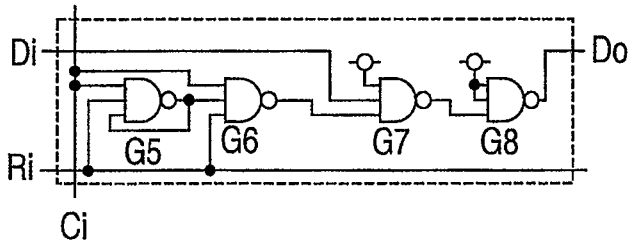


图 9（c）

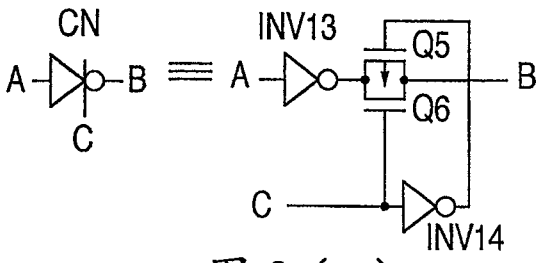


图 9（e）

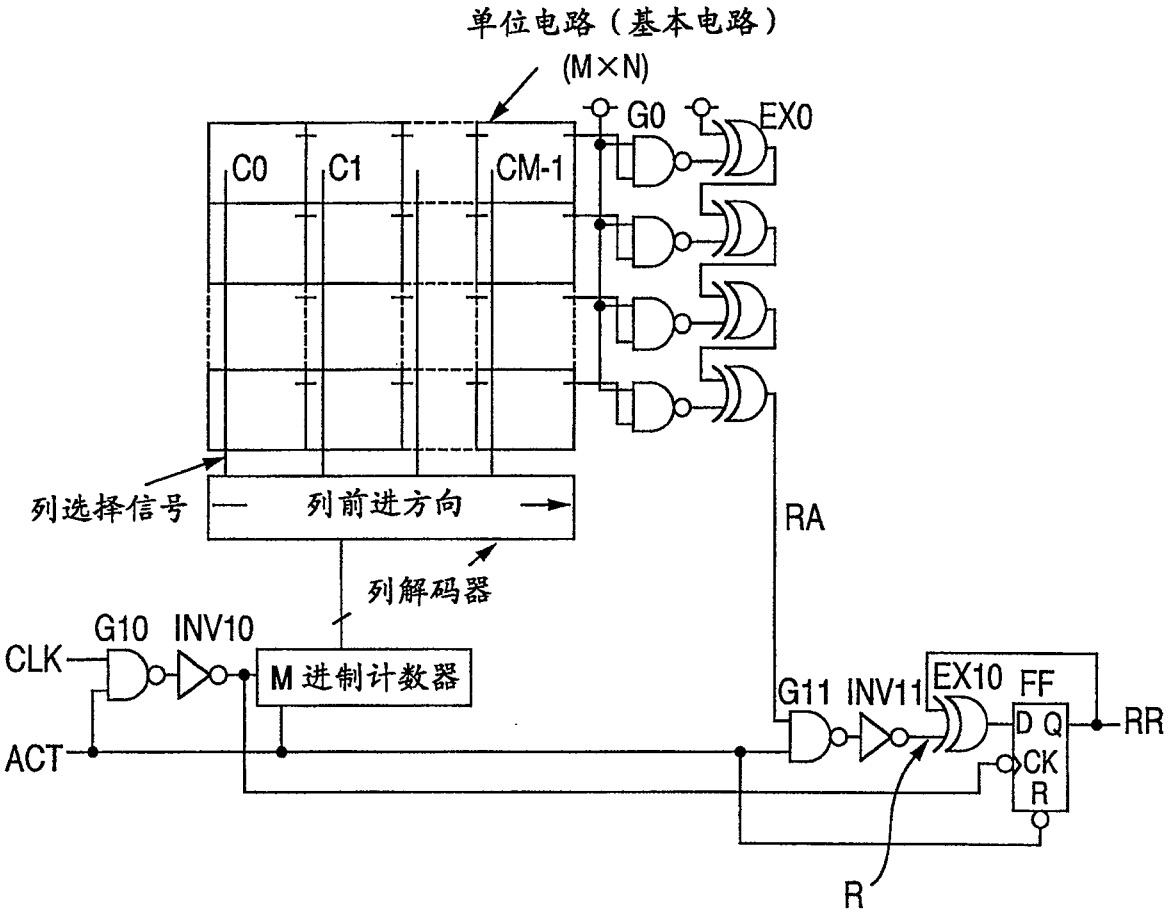

单位电路（基本电路）
(M×N)
G0
EX0
C0
C1
CM-1
列选择信号
列前进方向
RA
列解码器
G10
INV10
CLK
M进制计数器
ACT
G11
INV11
EX10
FF
D Q
CK
R
RR
R

图 10（a）

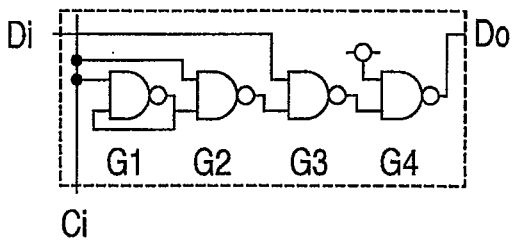

Di
Do
G1
G2
G3
G4
Ci

图 10（b）

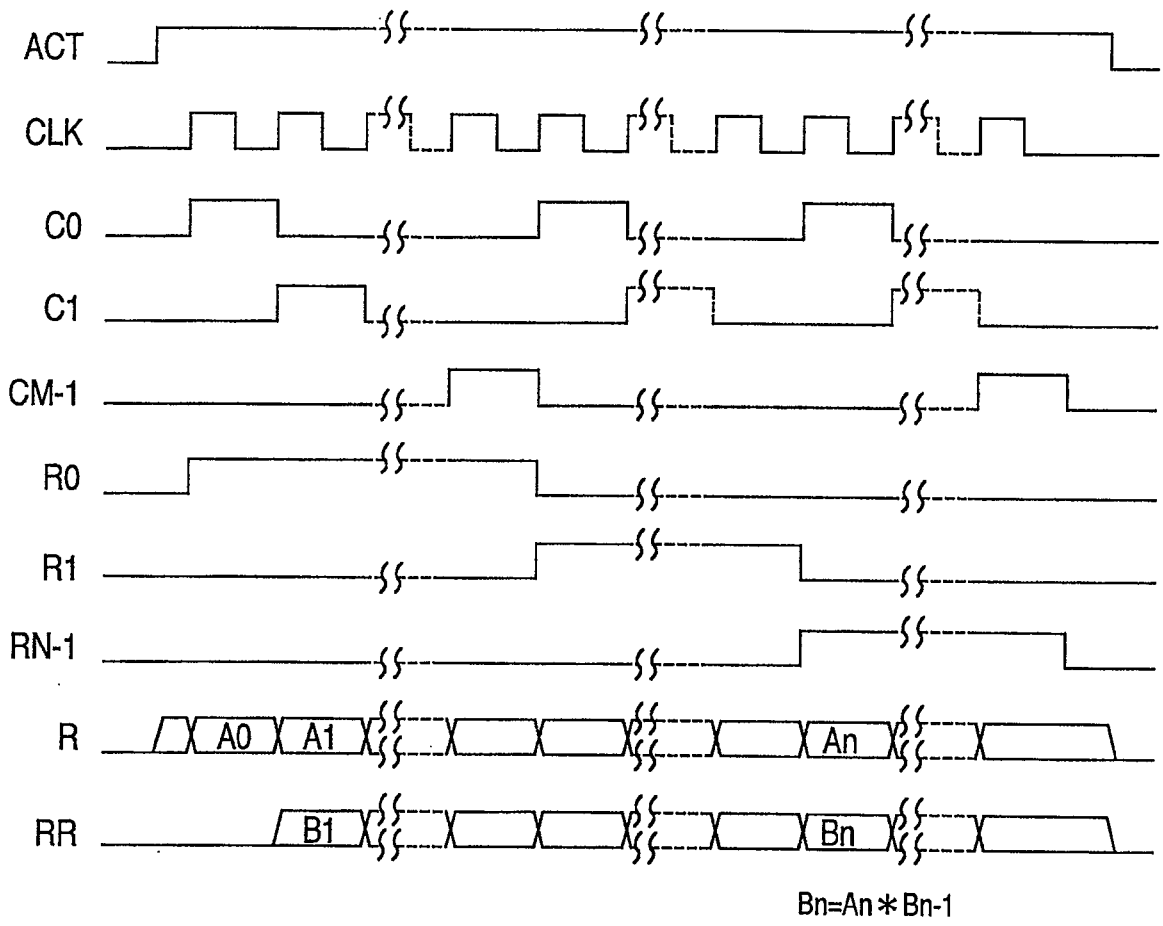

ACT
CLK
C0
C1
CM-1
R0
R1
RN-1
R
A0
A1
An
RR
B1
Bn
Bn=An＊Bn-1

图 11

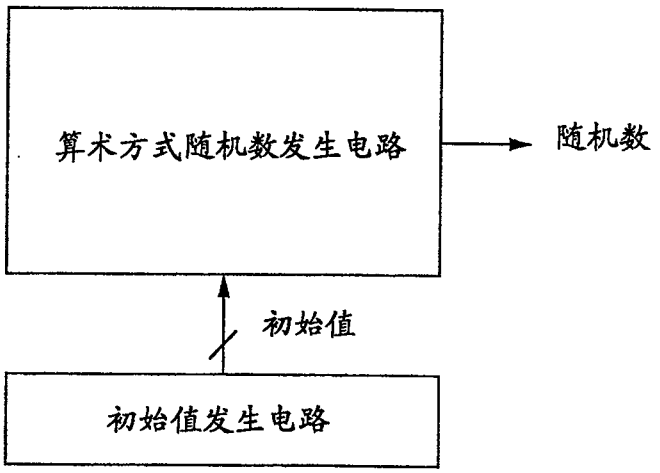

算术方式随机数发生电路
随机数
初始值
初始值发生电路

图 12

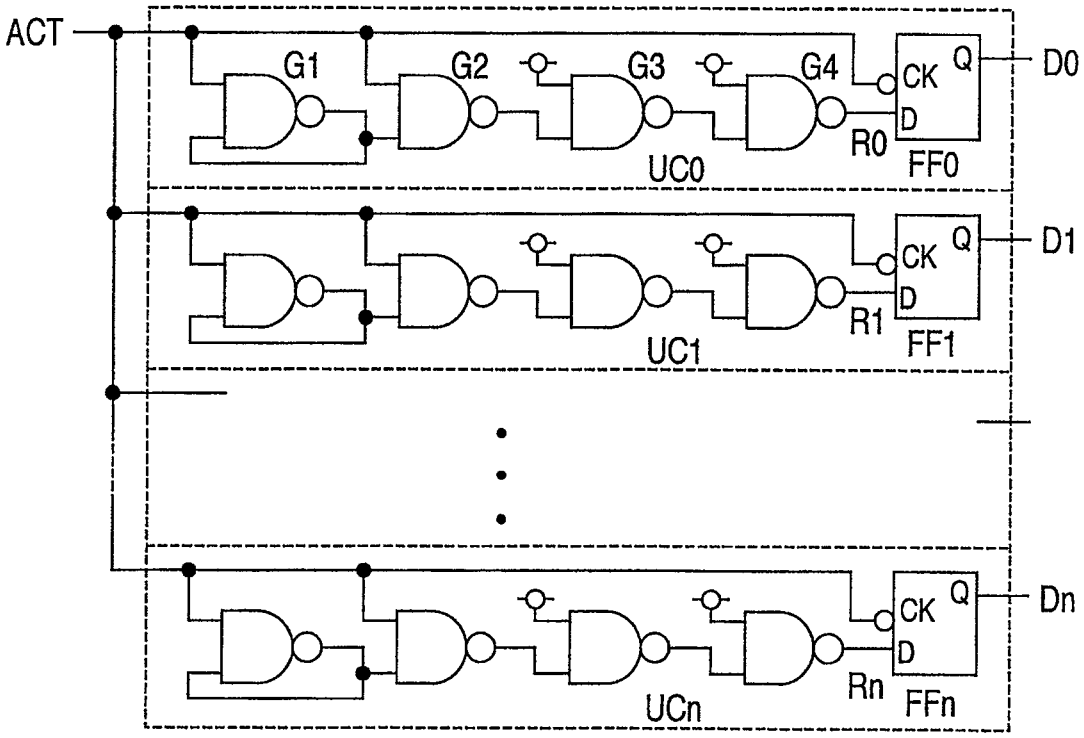

ACT
G1
G2
G3
G4
CK
Q
D
D0
R0
FF0
UC0
D1
R1
FF1
UC1
Dn
Rn
FFn
UCn

图 13

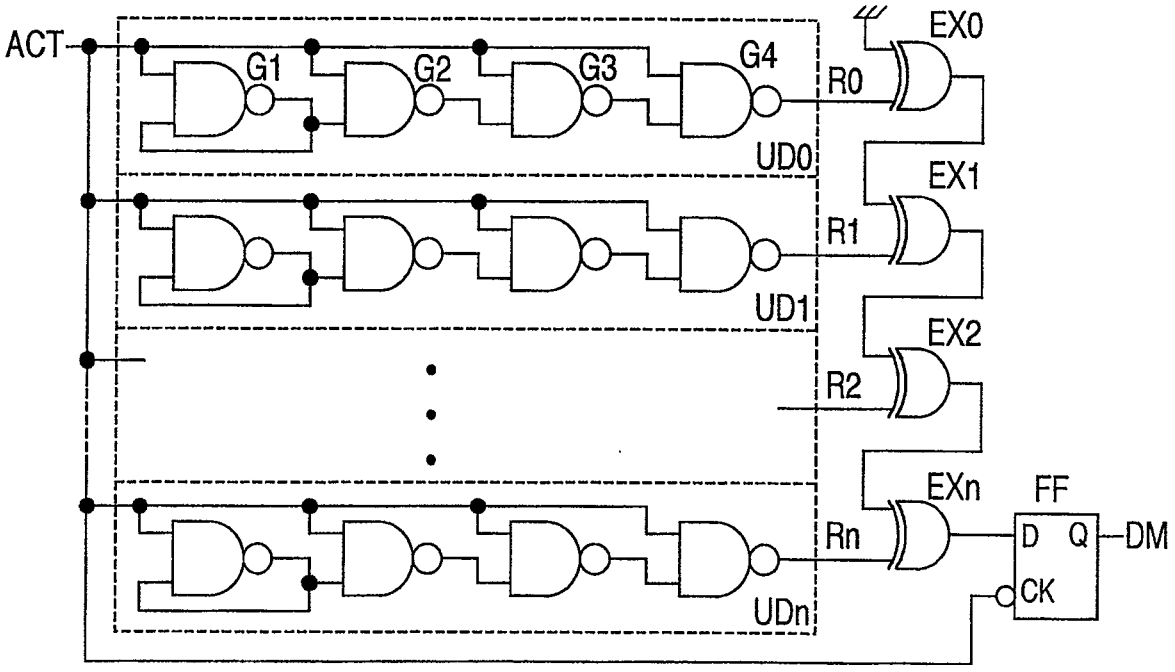

ACT
G1
G2
G3
G4
EX0
R0
UD0
EX1
R1
UD1
EX2
R2
EXn
FF
Rn
D
Q
DM
CK
UDn

图 14

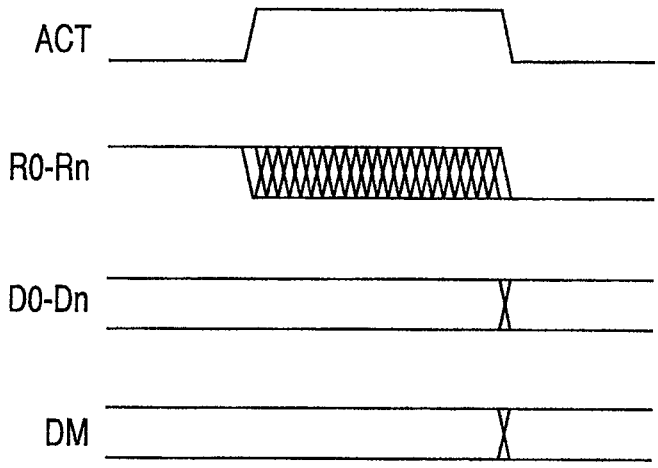

ACT
R0-Rn
D0-Dn
DM

图 15

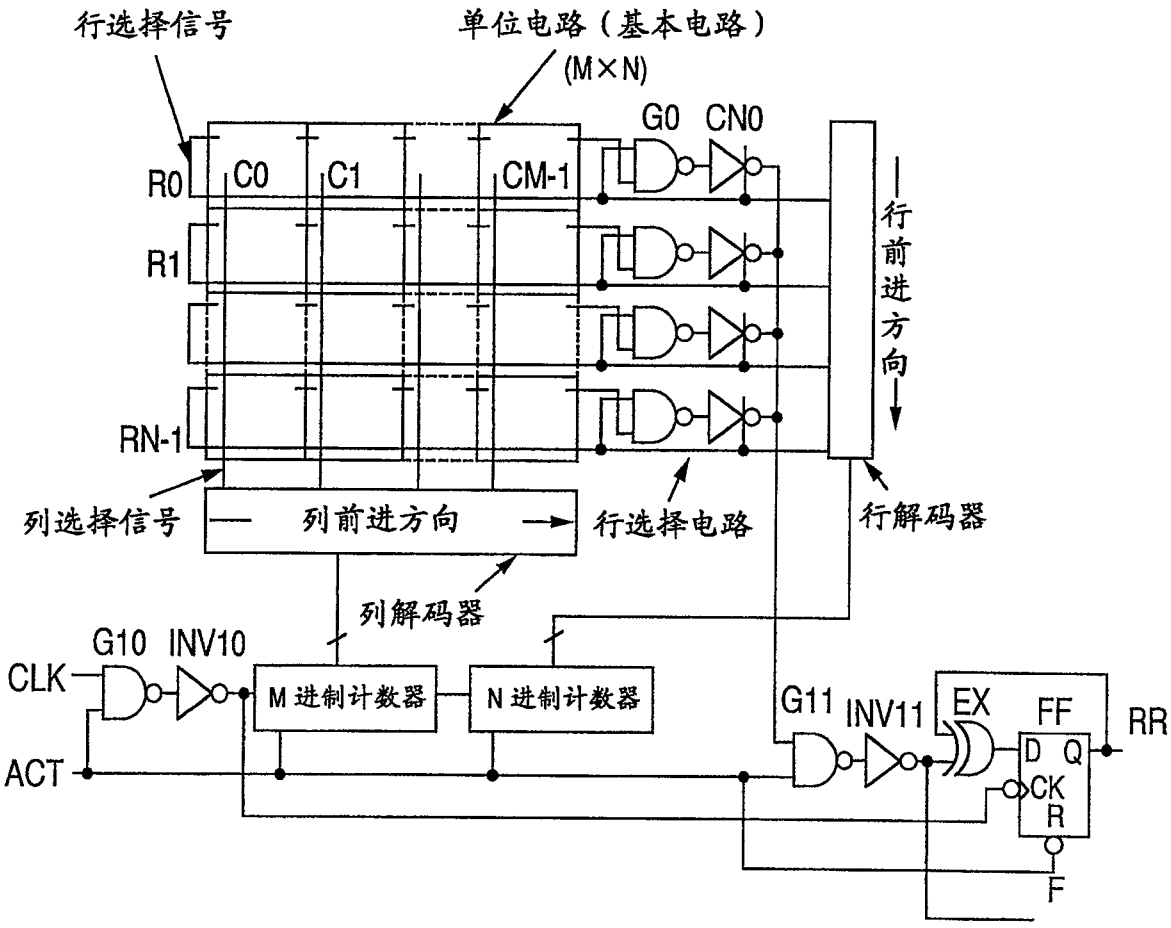

行选择信号
单位电路（基本电路）
(M×N)
G0
CN0
R0
C0
C1
CM-1
R1
RN-1
行前进方向
列选择信号
列前进方向
行选择电路
行解码器
列解码器
G10
INV10
CLK
ACT
M 进制计数器
N 进制计数器
G11
INV11
EX
FF
D
Q
CK
R
RR
F

图 16

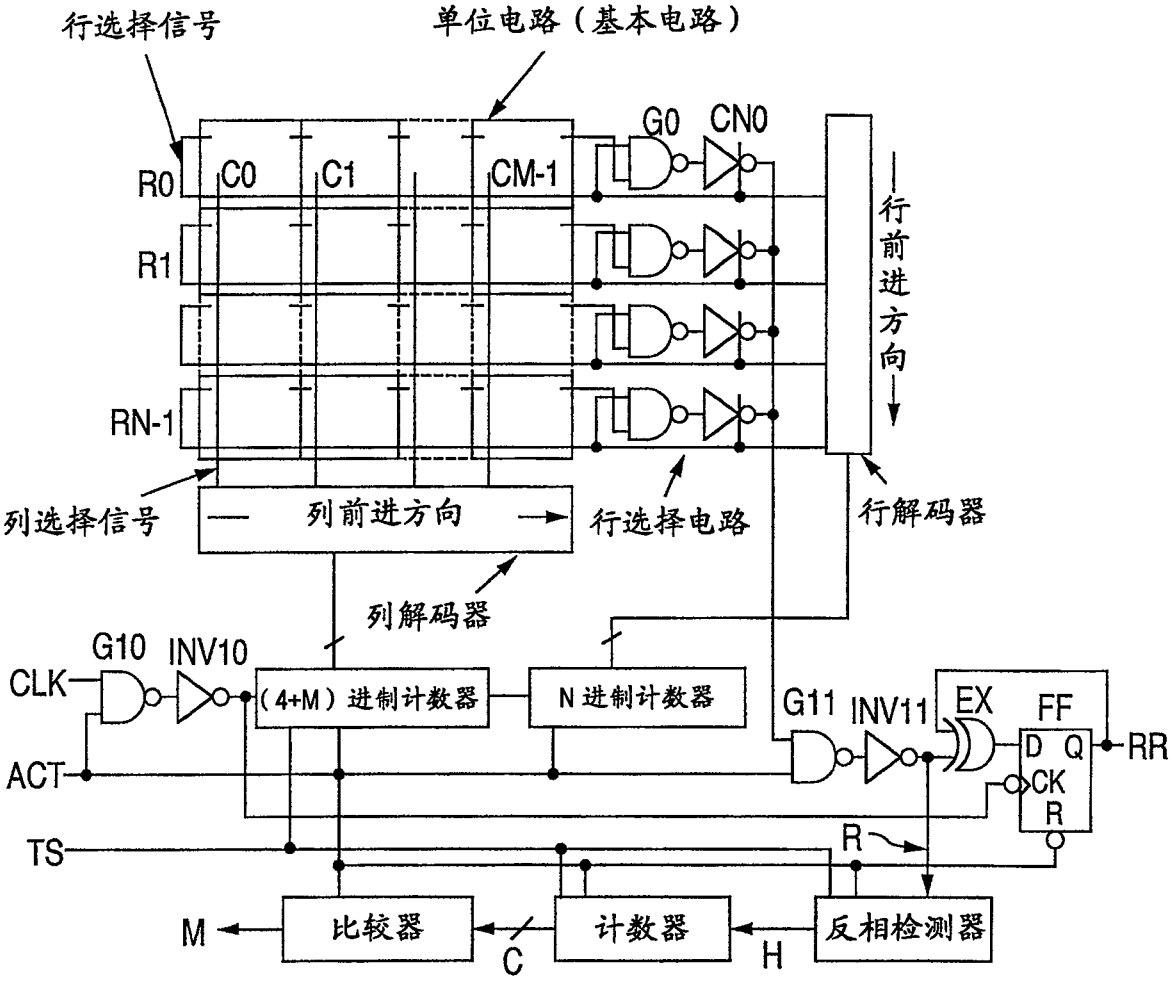

行选择信号
单位电路（基本电路）
G0
CN0
R0
C0
C1
CM-1
R1
RN-1
行前进方向
列选择信号
列前进方向
行选择电路
行解码器
列解码器
G10
INV10
CLK
(4+M)进制计数器
N进制计数器
G11
INV11
EX
FF
D Q
CK
R
RR
ACT
TS
R
M
比较器
C
计数器
H
反相检测器

图 17

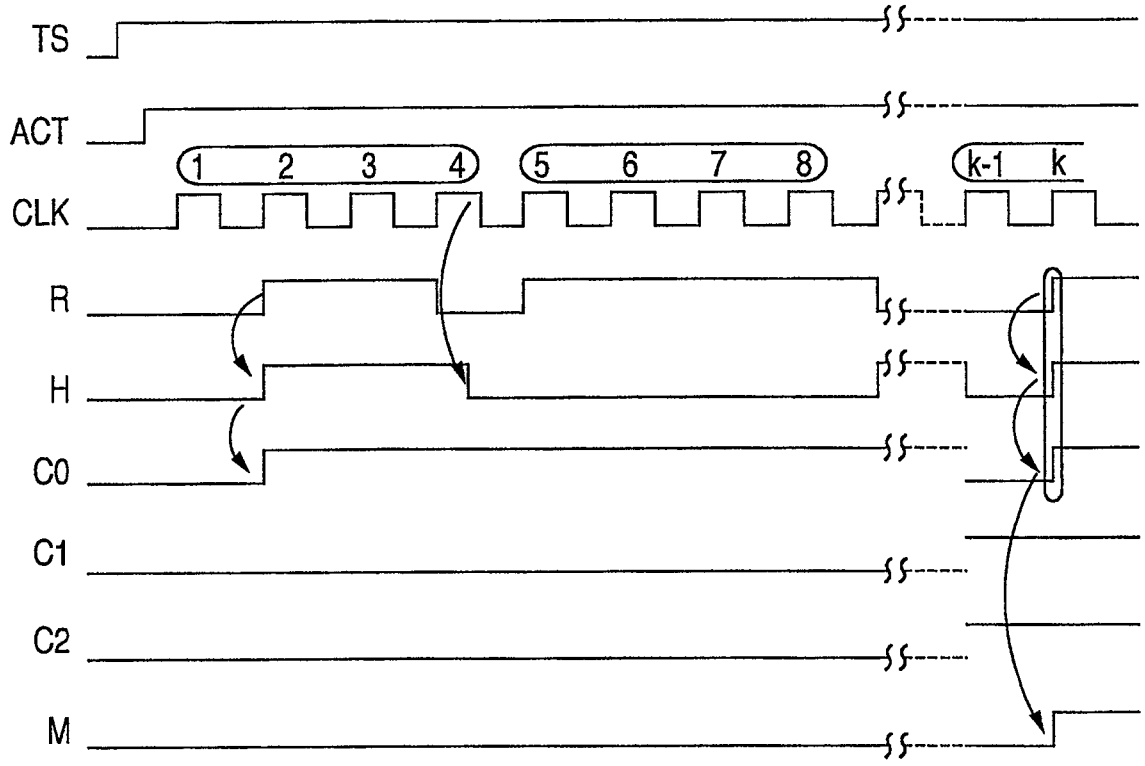

TS
ACT
CLK
1 2 3 4
5 6 7 8
k-1 k
R
H
C0
C1
C2
M

图 18

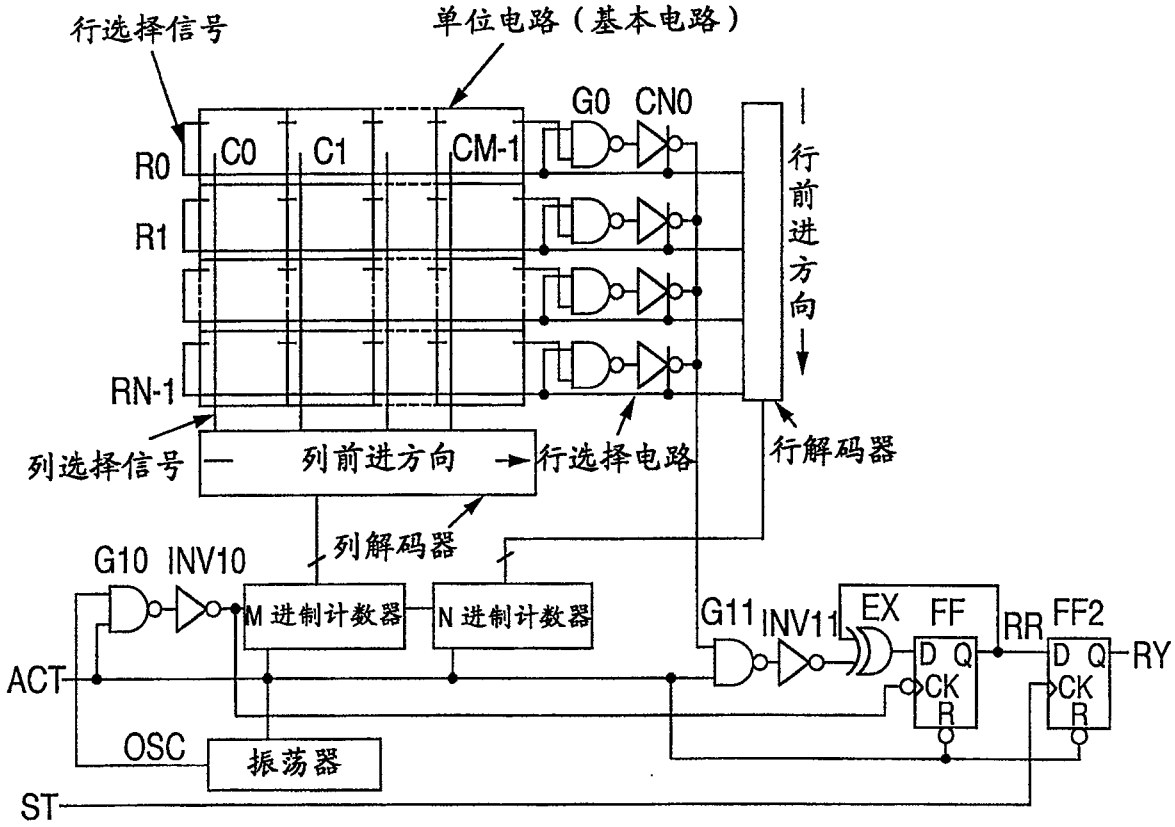

行选择信号
单位电路（基本电路）
G0 CN0
R0
C0 C1 CM-1
R1
RN-1
行前进方向
列选择信号
列前进方向
行选择电路
行解码器
列解码器
G10 INV10
M 进制计数器
N 进制计数器
G11 INV11
EX FF
RR FF2
RY
ACT
OSC
振荡器
ST

图 19

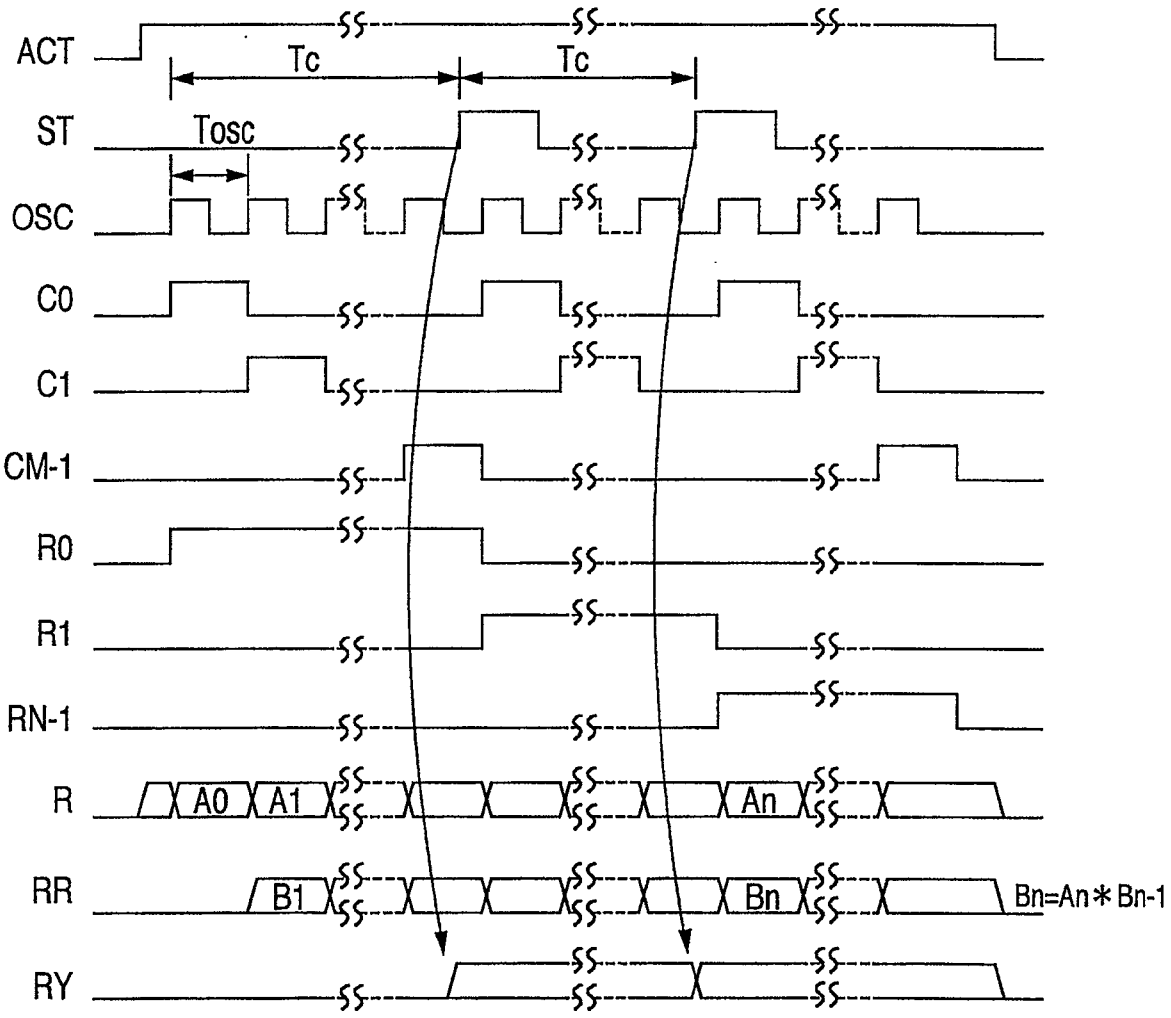

ACT
Tc
Tc
ST
Tosc
OSC
C0
C1
CM-1
R0
R1
RN-1
R
A0
A1
An
RR
B1
Bn
Bn=An＊Bn-1
RY

图 20

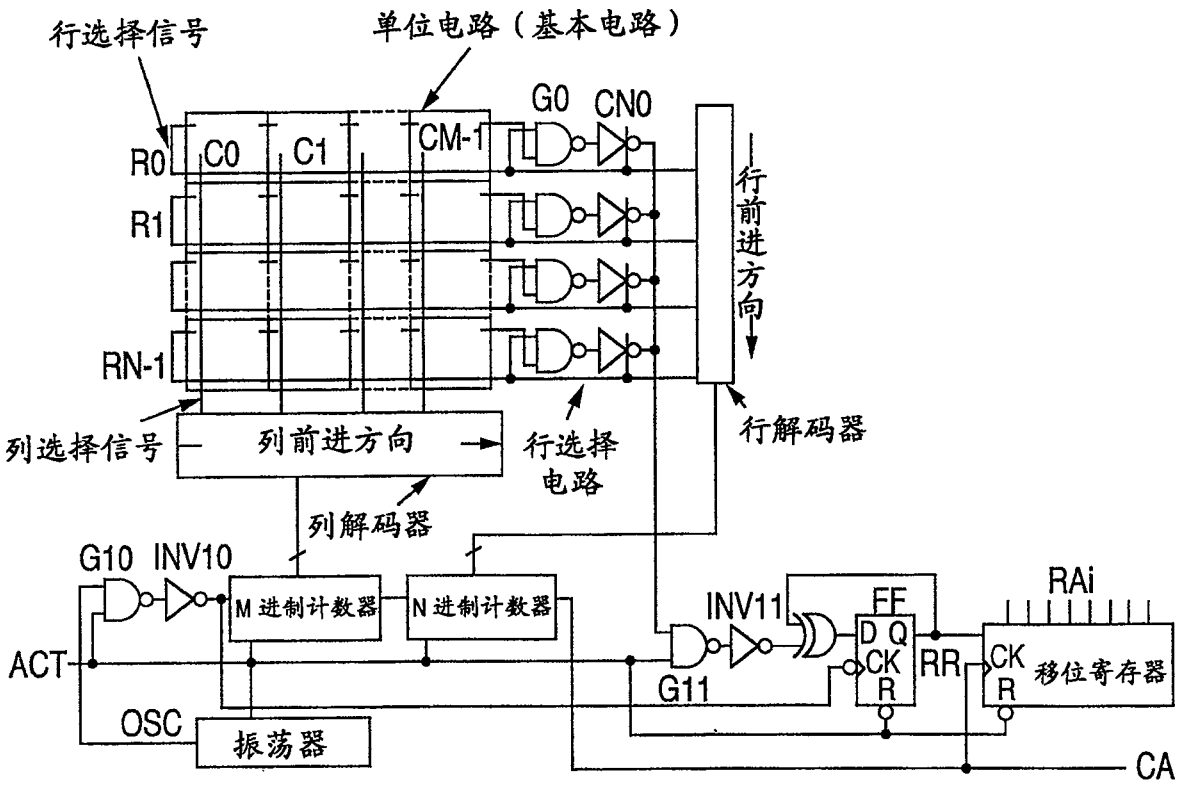

行选择信号
单位电路（基本电路）
G0
CN0
R0
C0
C1
CM-1
R1
RN-1
行前进方向
列选择信号
列前进方向
行选择电路
行解码器
列解码器
G10
INV10
M 进制计数器
N 进制计数器
INV11
FF
D Q
CK
R
RR
RAi
CK
R
移位寄存器
ACT
G11
OSC
振荡器
CA

图 21

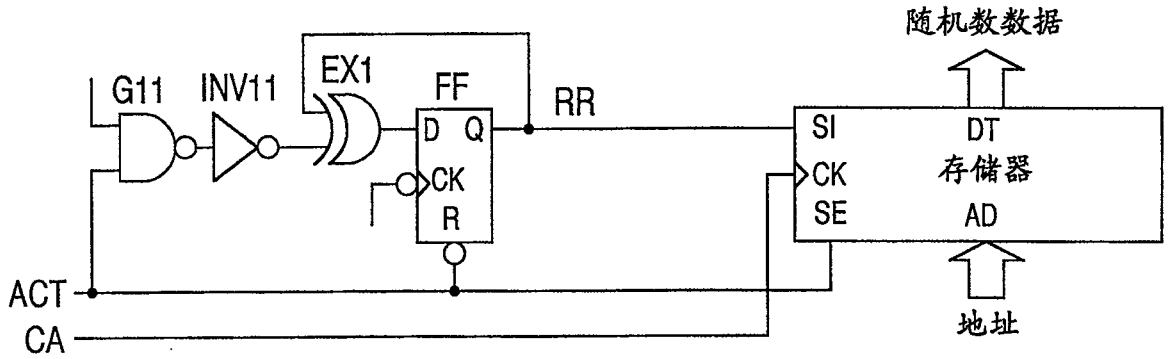

随机数数据
G11
INV11
EX1
FF
D Q
CK
R
RR
SI
CK
SE
DT
存储器
AD
ACT
CA
地址

图 22

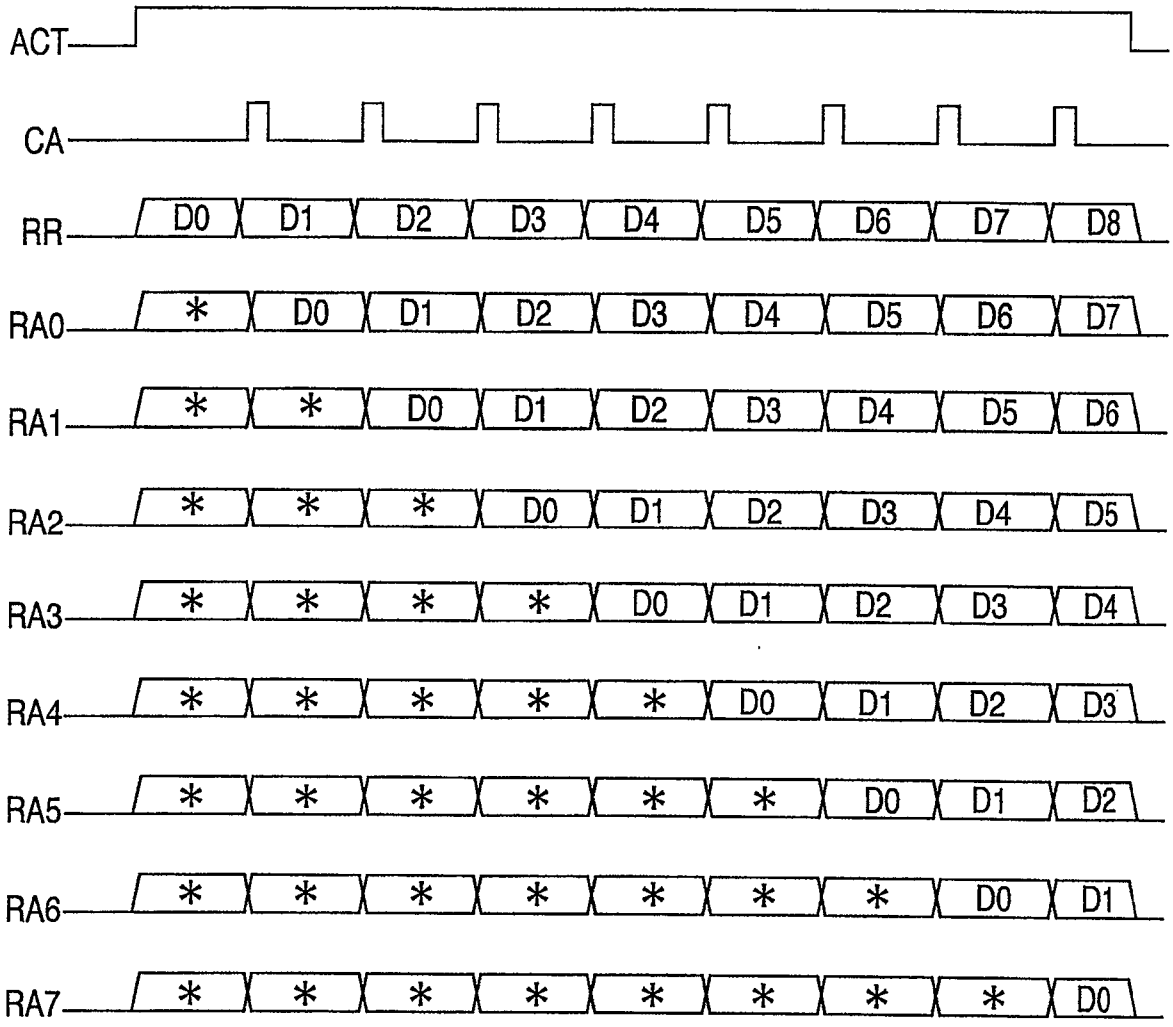

ACT
CA
RR
RA0
RA1
RA2
RA3
RA4
RA5
RA6
RA7
D0
D1
D2
D3
D4
D5
D6
D7
D8
*

图 23

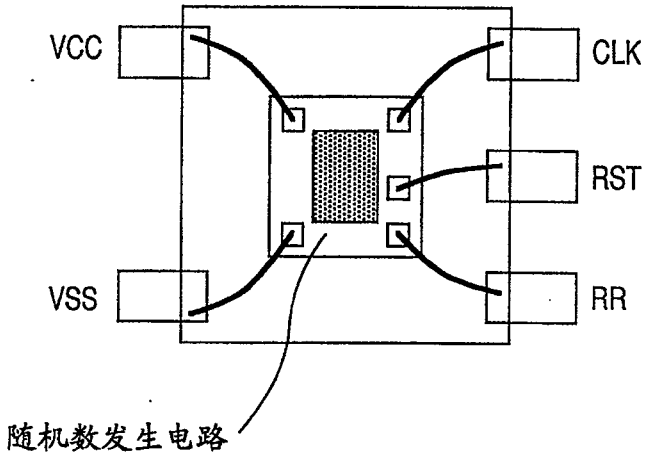

VCC
CLK
RST
VSS
RR
随机数发生电路

图 24

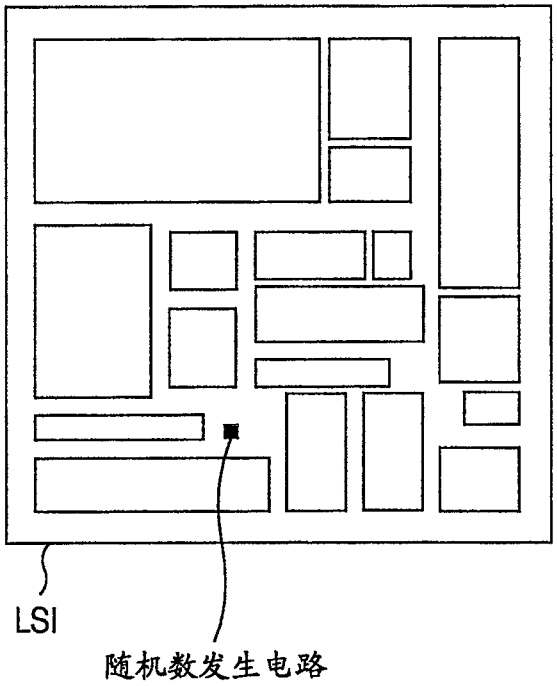


图 25

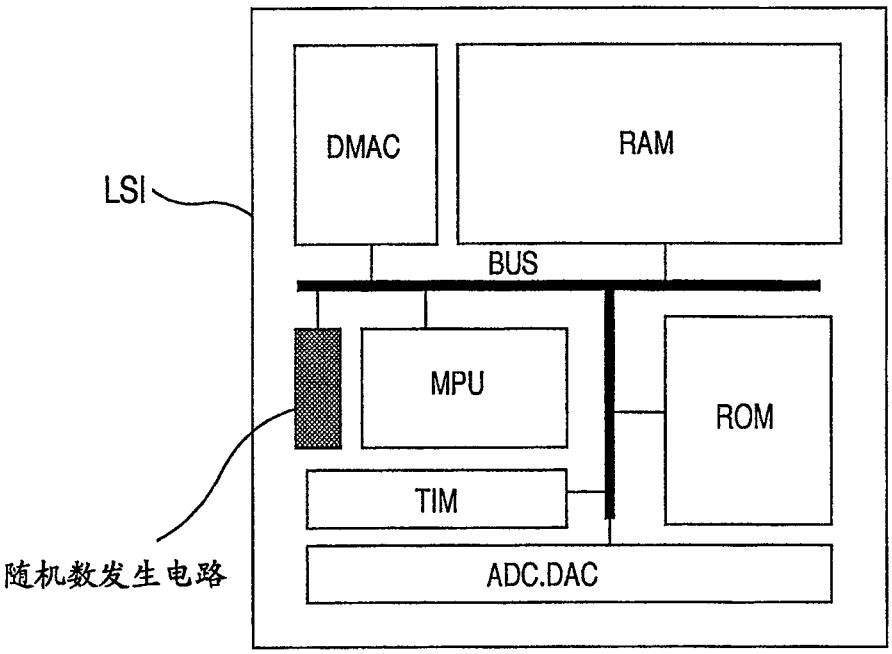


图 26

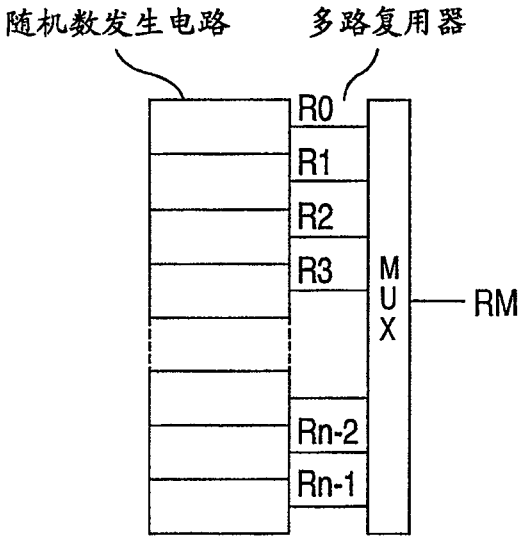


图 27（a）

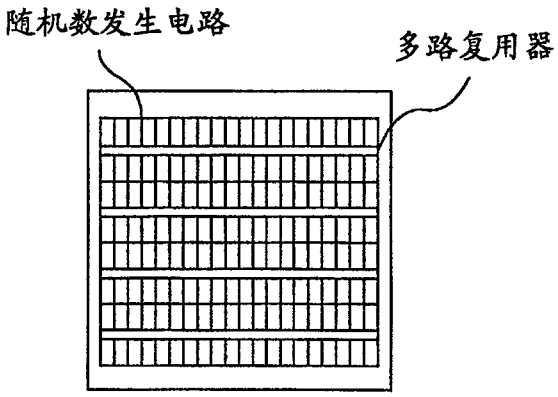


图 27（b）

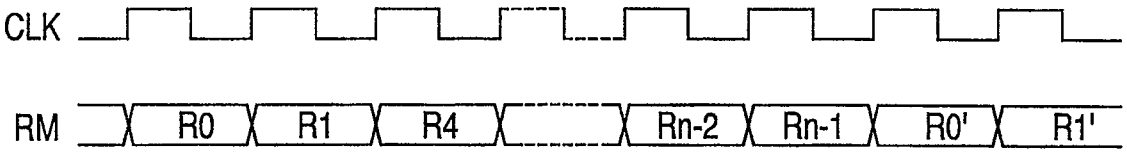


图 28

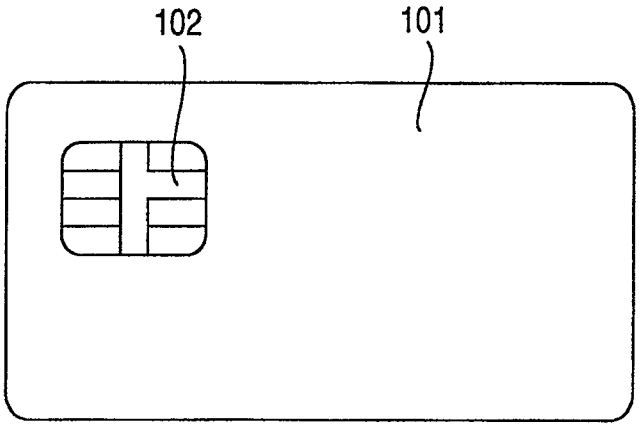

102
101

图 29

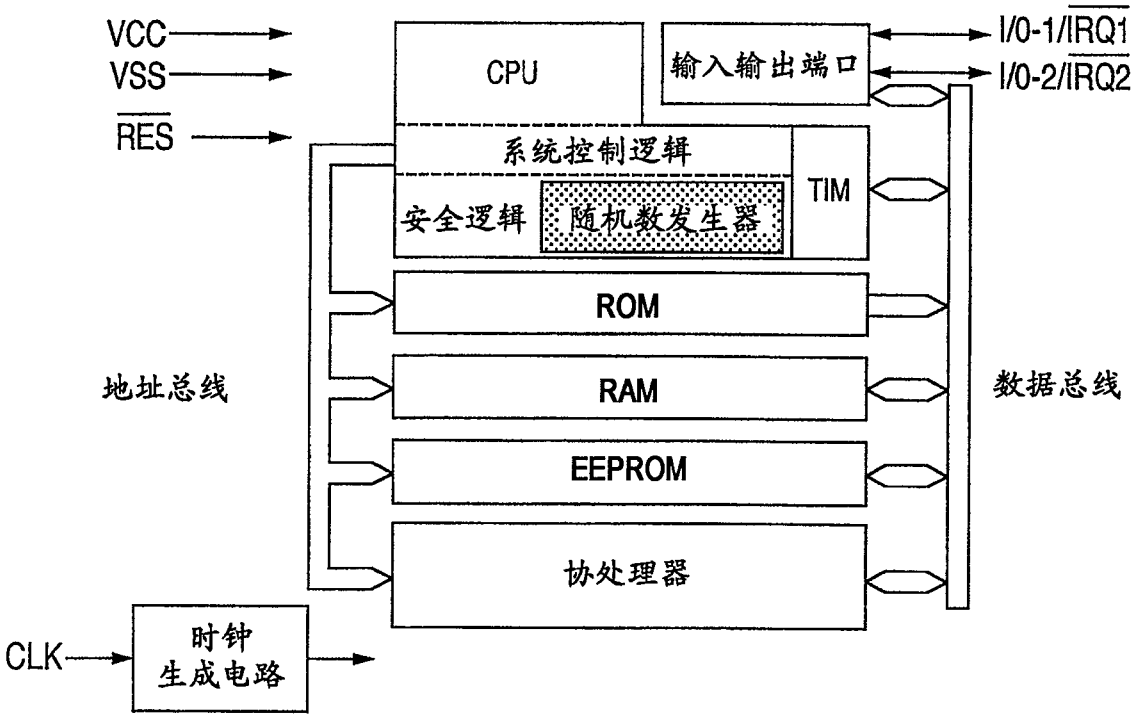

VCC
VSS
RES
CPU
输入输出端口
I/0-1/IRQ1
I/0-2/IRQ2
系统控制逻辑
TIM
安全逻辑
随机数发生器
ROM
RAM
EEPROM
协处理器
地址总线
数据总线
CLK
时钟
生成电路

图 30

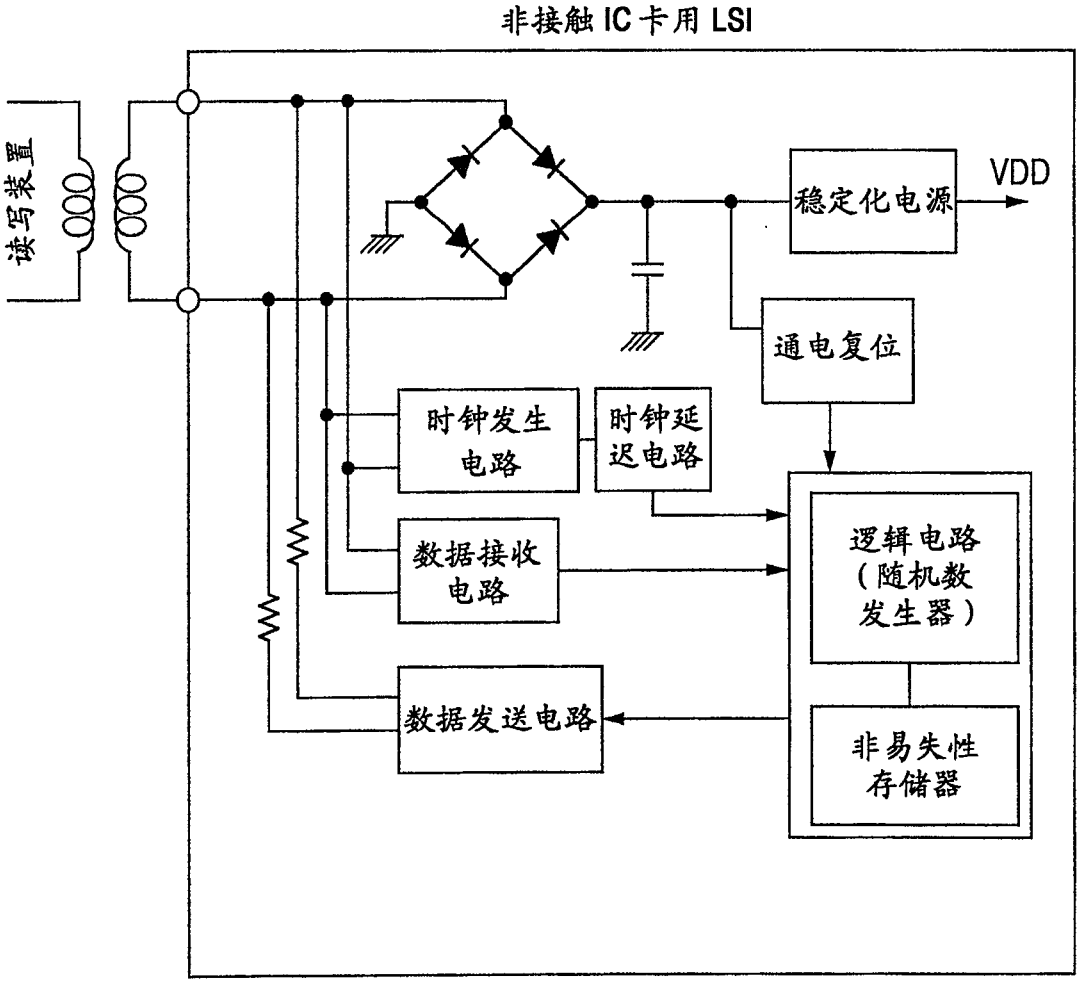

非接触IC卡用LSI
读写装置
稳定化电源
VDD
通电复位
时钟发生电路
时钟延迟电路
数据接收电路
逻辑电路（随机数发生器）
数据发送电路
非易失性存储器

图 31

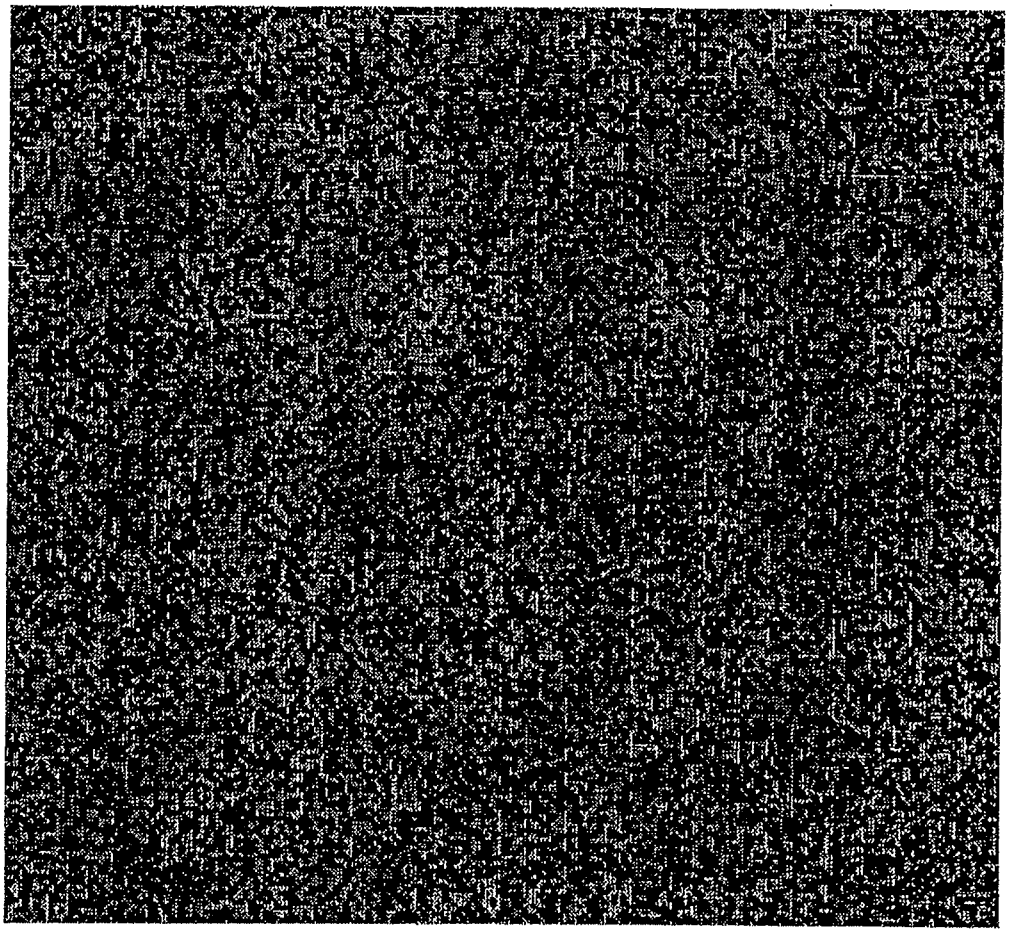


图 32

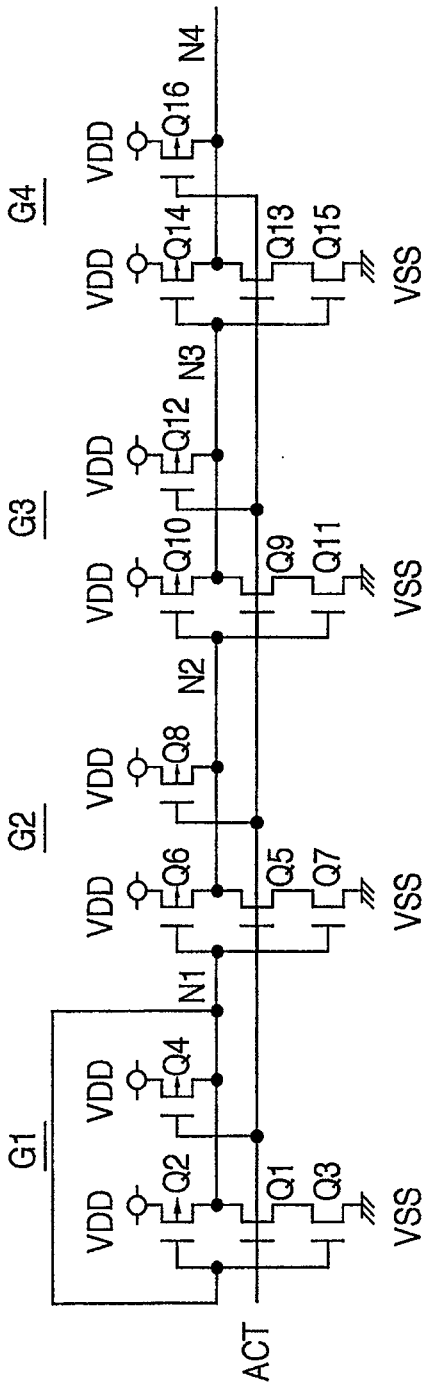

G1
G2
G3
G4
VDD
VSS
ACT
N1
N2
N3
N4
Q1
Q2
Q3
Q4
Q5
Q6
Q7
Q8
Q9
Q10
Q11
Q12
Q13
Q14
Q15
Q16

图 33(a)

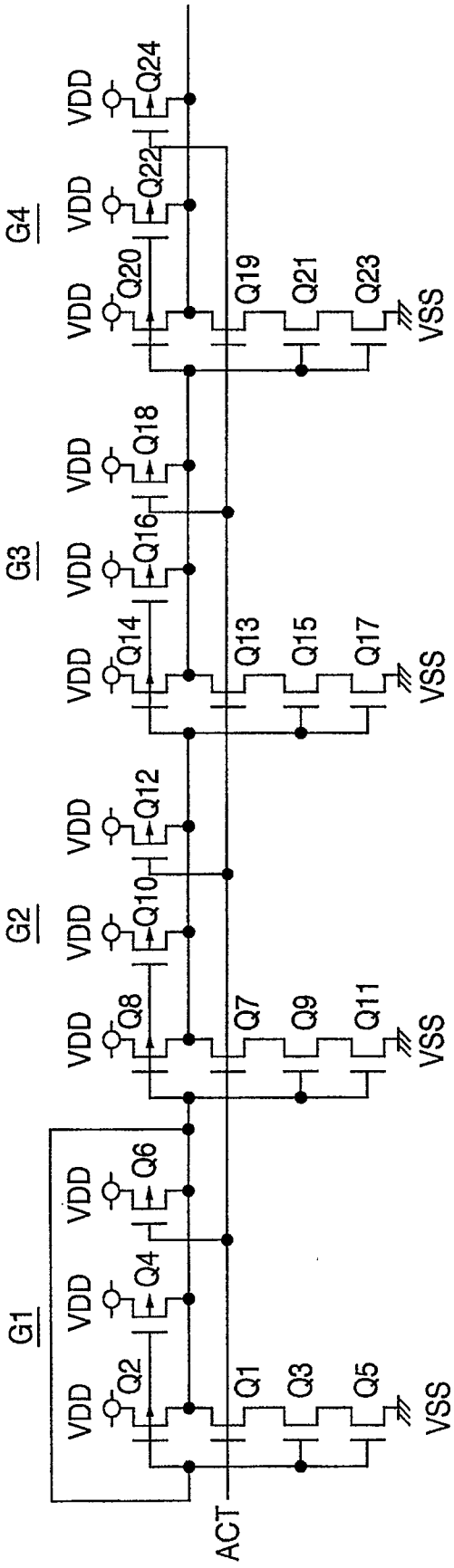

G1
G2
G3
G4
VDD
VSS
ACT
Q1
Q2
Q3
Q4
Q5
Q6
Q7
Q8
Q9
Q10
Q11
Q12
Q13
Q14
Q15
Q16
Q17
Q18
Q19
Q20
Q21
Q22
Q23
Q24

图 33 (b)

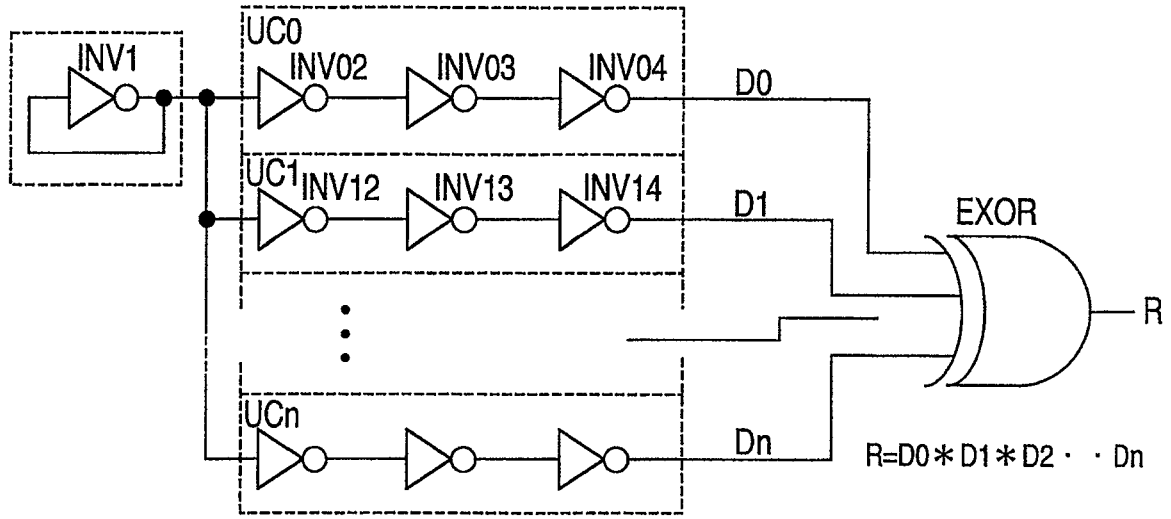

INV1
UC0
INV02
INV03
INV04
D0
UC1
INV12
INV13
INV14
D1
EXOR
R
UCn
Dn
R=D0＊D1＊D2・・Dn

图 34

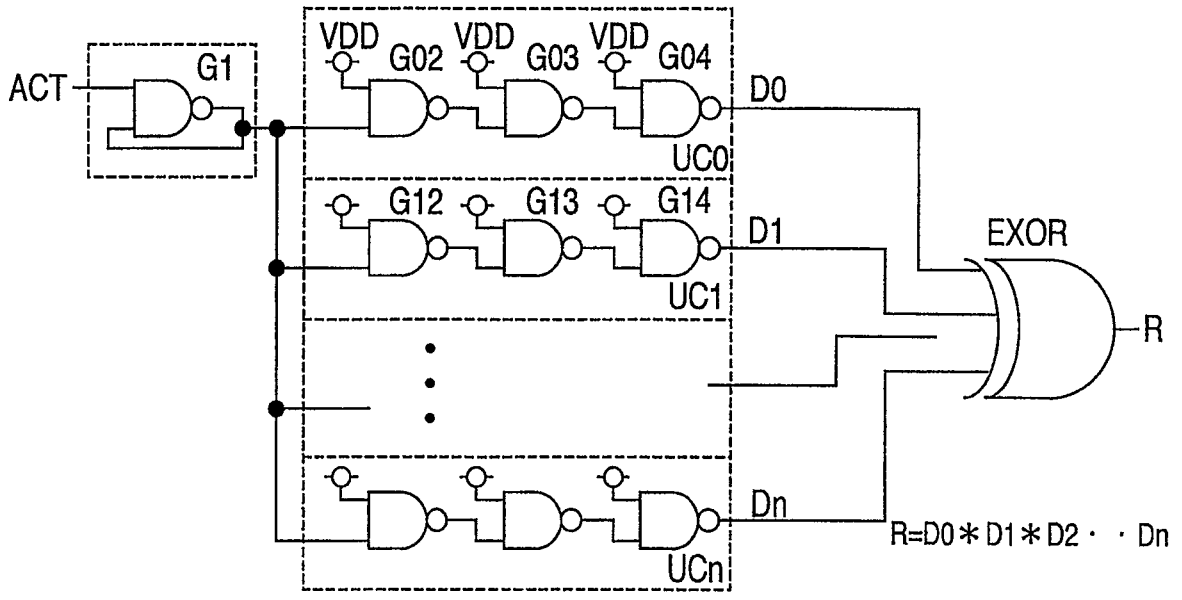

ACT
G1
VDD
G02
VDD
G03
VDD
G04
D0
UC0
G12
G13
G14
D1
EXOR
UC1
R
Dn
R=D0＊D1＊D2・・Dn
UCn

图 35